Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel

H. Hasse L. Schlesinger

PERIODICAL
GENERAL
LIBRARY

Wissenschaftlicher Beirat

H. Brandt / M. Dehn / G. Doetsch / A. Fraenkel / O. Haupt / F. Hausdorff
E. Hellinger / G. Kowalewski / H. Rademacher / K. Reidemeister
A. Rosenthal / C. Schaefer / W. Schmeidler / F. Schottky / O. Toeplitz

Band 160

Heft 2

Ausgegeben den 12. März 1929

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1929

Jährlich 8 Hefte. Vier Hefte bilden einen Band.

Band 160. Heft 2.

Inhaltsverzeichnis.

	Seite
Tietze, Heinrich, Bemerkungen über konvexe und nicht-konvexe Figuren	67
Brauer, Alfred, Über diophantische Gleichungen mit endlich vielen Lösungen . .	70
Prasad, Ganesh, On the differentiability of the integral function	100
Burstin, C. und **Mayer, W.,** Distributive Gruppen von endlicher Ordnung . . .	111

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgend einem Grunde Text-Änderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion ausschließlich unter der Adresse
An die Redaktion des Journals für die reine und angewandte Mathematik
Professor Dr. Kurt Hensel, Marburg (Bez. Cassel), Behringweg 7.

Bemerkungen über konvexe und nicht-konvexe Figuren.

Von *Heinrich Tietze* in München.

1. Mit dem Gegenstand meiner Note über konvexe Figuren [1]) nahe verwandt sind von *Leja* und *Wilkosz* [2]) schon vor einigen Jahren veröffentlichte Betrachtungen, von denen ich erst jetzt Kenntnis erhalten habe. Gelegentlich dieses nachträglichen Literaturverweises sei es mir gestattet, eine durch die Lektüre jener Arbeit angeregte Verallgemeinerung meines früheren Ergebnisses mitzuteilen.

Der in Nr. 2 und 5 meiner Note, l. c. [1]), bewiesene Satz läßt sich folgendermaßen aussprechen: Ist $\mathfrak{D}_0$ eine ebene zusammenhängende offene Menge, $\mathfrak{M}$ ihre abgeschlossene Hülle, ferner $\mathfrak{D}$ ($\geqq \mathfrak{D}_0$) die Menge der inneren Punkte von $\mathfrak{M}$ und ist $\mathfrak{D}$ *nicht konvex* (oder, was dasselbe heißt, ist $\mathfrak{M}$ nicht konvex), dann gibt es auf der Begrenzung $\mathfrak{L} = \mathfrak{M} - \mathfrak{D}$ von $\mathfrak{D}$ mindestens einen Punkt, durch den keine Stützstrecke an $\mathfrak{D}$ geht. Mittels analoger Überlegungen läßt sich, wie in Nr. 2 geschehen soll, der folgende etwas weitergehende Satz beweisen [3]):

Satz (A): *Ist $\mathfrak{D}_0$ eine ebene zusammenhängende offene nichtkonvexe Menge, dann gibt es auf der Begrenzung von $\mathfrak{D}_0$ mindestens einen Punkt Z_0, durch den keine Stützstrecke an $\mathfrak{D}_0$ geht.*

Mit Mengen, die den gleichen Voraussetzungen genügen, wie $\mathfrak{D}_0$ im Satz (A), haben sich nun *Leja* und *Wilkosz* beschäftigt. Sie bezeichnen als *Konkavitätsstelle* einer ebenen offenen Punktmenge $\mathfrak{D}$ einen solchen Punkt $X_0 = (x_1^0, x_2^0)$ auf der Begrenzung von $\mathfrak{D}$, daß für eine geeignete durch X_0 gehende Gerade $\sum_1^2 a_i(x_i - x_i^0) = 0$ und ein geeignetes $r > 0$ alle den beiden Ungleichungen

$$\sum_1^2 a_i(x_i - x_i^0) \leqq 0 \quad \text{und} \quad 0 < \sum_1^2 (x_i - x_i^0)^2 \leqq r^2$$

genügenden Punkte zu $\mathfrak{D}$ gehören. (Ganz analog lautet die Definition für Mengen im n-dimensionalen Raum). *Leja* und *Wilkosz* beweisen dann den Satz, daß in der *Ebene* jede zusammenhängende offene nicht-konvexe Punktmenge $\mathfrak{D}_0$ wenigstens einen Konkavitätspunkt X_0 besitzt. Darin liegt mehr als das Nichtvorhandensein einer Stützstrecke an $\mathfrak{D}_0$ durch X_0 (wie es Satz (A) für mindestens einen Punkt der Begrenzung behauptet); z. B. ist für die Vereinigung der zwei Mengen, die durch $x_1 > 0$ bzw. durch $x_2 > 0$, $x_1 > -x_2^2$ definiert sind, der Punkt (0, 0) zwar ein Punkt ohne Stützstrecke, aber kein Konkavitätspunkt [4]). Während sich aber Satz (A) auf mehr Dimensionen

[1]) Dieses Journal, Bd. 158 (1927), S. 168. (Vgl. dazu auch eine demnächst erscheinende Note von *K. Reinhardt* im Jahresber. D. M.-V. [Zusatz bei d. Korr.]).

[2]) Sur une propriété des domaines concaves, Annales de la Soc. polon. de math., t. 2 (1923), Kraków 1924, p. 222.

[3]) Daß dieser Satz (A) über den vorgenannten l. c. [1]) bewiesenen Satz hinausgeht, zeigt etwa das Beispiel (vgl. l. c. [1]), p. 169, Anm. 2) derjenigen Menge $\mathfrak{D}_0$, die aus allen Punkten $x_1^2 + x_2^2 < 1$ mit Ausnahme der Punkte $x_2 = 0$, $0 \leqq x_1 < 1$ besteht. (Der Punkt $x_1 = 0$, $x_2 = 0$ ist hierbei ein Punkt ohne Stützstrecke an $\mathfrak{D}_0$).

[4]) Der Punkt (0, 0) ist übrigens wenigstens ein „schwacher Konkavitätspunkt" im Sinn des Zusatzes zu Nr. 1. Ein Beispiel eines Punktes ohne Stützstrecke, der auch nicht schwacher Konkavitätspunkt ist, erhält man in dem Punkt (0, 0), wenn man für $\mathfrak{D}_0$ die Menge $x_2 > \lim_{t \to x_1} t^2 \sin \frac{1}{t}$ nimmt.

übertragen läßt (s. Nr. 4), verliert der Satz von *Leja* und *Wilkosz*, wie die Verfasser ausdrücklich hervorheben, in Räumen $\mathfrak{R}^n$ von $n > 2$ Dimensionen seine Gültigkeit (z. B. hat im $\mathfrak{R}^3$ die nicht-konvexe Vereinigung der beiden Mengen $x_1^2 + x_2^2 + x_3^2 < 1$ und $(x_1 - 1)^2 + x_2^2 + x_3^2 < 1$ keinen Konkavitätspunkt).

Zusatz [5]). Man kann die gegenseitige Beziehung der Begriffe „Stützstrecke" und „Konkavitätspunkt" vielleicht am deutlichsten folgendermaßen kennzeichnen: Ist $\mathfrak{M}$ eine Menge [6]) des n-dimensionalen Raumes $\mathfrak{R}^n$, so heiße ein Punkt X_0 der Begrenzung von $\mathfrak{M}$ 1. ein schwacher Konvexitätspunkt, 2. ein starker Konvexitätspunkt, 3. ein schwacher Konkavitätspunkt, 4. ein starker Konkavitätspunkt, wenn es ein $r > 0$ und durch $X_0 = (x_1^0, \ldots, x_n^0)$ eine Ebene $L \equiv \Sigma a_i(x_i - x_i^0) = 0$ gibt, sodaß von den der Ungleichung $0 < \Sigma (x_i - x_i^0)^2 \leqq r^2$ genügenden Punkten 1. kein Punkt mit $L > 0$ zu $\mathfrak{M}$ gehört, 2. kein Punkt mit $L \geqq 0$ zu $\mathfrak{M}$ gehört, 3. alle Punkte mit $L < 0$ zu $\mathfrak{M}$ gehören, 4. alle Punkte mit $L \leqq 0$ zu $\mathfrak{M}$ gehören. Die schwachen Konvexitätspunkte sind dann die Punkte mit Stützscheibe (bzw. Stützstrecke für $n = 2$), die starken Konkavitätspunkte sind die Konkavitätspunkte im Sinne von *Leja* und *Wilkosz*. Satz (A) in seiner Verallgemeinerung auf n Dimensionen besagt für eine nicht-konvexe zusammenhängende offene Menge $\mathfrak{O}_0$, daß nicht alle ihre Begrenzungspunkte schwache Konvexitätspunkte sein können. Der Satz von *Leja* und *Wilkosz* besagt für $n = 2$ (und nur für $n = 2$) darüber hinaus, daß mindestens ein starker Konkavitätspunkt auftreten muß.

2. Wir kommen zum Beweis von Satz (A). Sei $\mathfrak{K}_0$ die konvexe Hülle von $\mathfrak{O}_0$, also ebenso wie $\mathfrak{O}_0$ eine offene Menge. Nach Voraussetzung ist $\mathfrak{K}_0 \neq \mathfrak{O}_0$; sei P ein Punkt von $\mathfrak{K}_0 - \mathfrak{O}_0$. Man zeigt dann leicht, daß unter den von P ausgehenden Halbstrahlen t diejenigen, die von Punkten von $\mathfrak{O}_0$ frei sind, falls solche vorhanden sind, stets einen Winkel $\geqq 0$ und $< \pi$ erfüllen [7]), daß es also durch P eine solche Gerade g gibt, die auf jedem ihrer Halbstrahlen g_1, g_2 Punkte von $\mathfrak{O}_0$ enthält. Ist dann A_1 bzw. A_2 ein Punkt von $\mathfrak{O}_0$ auf g_1 bzw. g_2, s ein einfacher Streckenzug in $\mathfrak{O}_0$ von A_1 nach A_2, so darf angenommen werden, daß s zusammen mit der Strecke A_1A_2 ein einfaches Polygon q bildet (nachdem man nötigenfalls A_1, A_2 durch geeignete Treffpunkte von s mit g ersetzt hat). Sei ferner PP'' ein Lot auf g, das (bis auf den Punkt P) ganz im Innern des Polygons q liegt, und sei $\mathfrak{Q}$ die Menge der Punkte von $\mathfrak{K}_0 - \mathfrak{O}_0$, die im Innern von q und auf derjenigen Seite von g liegen, auf der P'' liegt. Falls nun die Menge $\mathfrak{Q}$

---

[5]) Zusatz bei der Korrektur.

[6]) $\mathfrak{M}$ muß dabei nicht als offene Menge vorausgesetzt werden.

[7]) Man erkennt dies, wie l. c. [1]) Nr. 5, indem man von einem von $\mathfrak{O}_0$ freien Halbstrahl $t = t_0$ durch P ausgeht und ihn um P in beiden Richtungen soweit dreht, als dies möglich ist, ohne $\mathfrak{O}_0$ zu treffen: außerhalb des so erhaltenen Winkels kann es keine anderen von $\mathfrak{O}_0$ freien Halbstrahlen durch P geben, weil sonst $\mathfrak{O}_0$ nicht zusammenhängend wäre; und der fragliche Winkel muß $< \pi$ sein, weil sonst P nicht der konvexen Hülle von $\mathfrak{O}_0$ angehören würde. (Diese Überlegung gilt ganz unabhängig davon, ob die Begrenzung von $\mathfrak{K}_0$ vollständig zur Begrenzung von $\mathfrak{O}_0$ gehört oder nicht. Ebenso sieht man, daß auch bei dem l. c. [1]) gegebenen Beweis die für die dort mit $\mathfrak{M}$, $\mathfrak{N}$, $\mathfrak{K}$ bezeichneten Mengen gemachte Unterscheidung in die beiden Fälle I und II, je nachdem die Begrenzung von $\mathfrak{K}$ vollständig zu derjenigen von $\mathfrak{M}$ gehört oder nicht, entbehrlich ist und daß allemal das für den Fall II l. c. in Nr. 5 angegebene Beweisverfahren anwendbar ist, unter P einen nicht zu $\mathfrak{M}$ gehörigen Punkt im Inneren von $\mathfrak{K}$ verstanden. Diese Bemerkung ist insbesondere von Belang für den Fall [der sonst eine Modifikation des Beweisverfahrens l. c. Nr. 2, Fall I erfordern würde] daß bei einer nicht-beschränkten Menge $\mathfrak{M}$ die Begrenzung von $\mathfrak{K}$ nicht vollständig zu $\mathfrak{M}$ gehört, dabei aber keine *Strecke* auf der Begrenzung von $\mathfrak{K}$ existiert, deren innere Punkte in $\mathfrak{R}$ und deren Endpunkte auf $\mathfrak{M}$ liegen, sondern statt dessen eine oder zwei *Halbgerade*. Ein solcher Fall liegt z. B. vor für die durch $x_1 \geqq 1$, $|x_1 x_2| \leqq 1$ gegebene Menge $\mathfrak{M}$; hier ist $\mathfrak{K}$ durch $x_1 \geqq 1$, $|x_2| \leqq 1$ gegeben und die Begrenzung von $\mathfrak{K}$ enthält die nicht zu $\mathfrak{M}$ gehörenden Halbgeraden $x_1 > 1$, $x_2 = \pm 1$.)

nicht leer ist ($\mathfrak{Q} > 0$), dann sind die Punkte Z von $\mathfrak{Q}$, die am weitesten von g entfernt liegen (solcher Punkte Z kann es einen oder mehrere geben), sicher Randpunkte von $\mathfrak{D}_0$ (nicht etwa Innenpunkte von $\mathfrak{K}_0 - \mathfrak{D}_0$, da es sonst unter den Punkten von $\mathfrak{K}_0 - \mathfrak{D}_0$ im Inneren von q auf der fraglichen Seite von g noch weiter von g entfernte gäbe). Unter diesen Punkten Z findet man dann so wie l. c.[1]) Nr. 2 (Fall II) einen Punkt Z_0, durch den keine Stützstrecke an $\mathfrak{D}_0$ geht, womit Satz (A) im Falle $\mathfrak{Q} > 0$ bewiesen ist. Ist aber $\mathfrak{Q}$ leer ($\mathfrak{Q} = 0$), d. h. gehören alle Punkte im Inneren von q und auf derselben Seite von g wie P'' zu $\mathfrak{D}_0$, dann wird unter allen Punkten von $\mathfrak{K}_0 - \mathfrak{D}_0$, die auf der Strecke A_1A_2 liegen (zu denen sicherlich P gehört), der an A_1 nächstgelegene ein Punkt Z_0 sein, durch den keine Stützstrecke an $\mathfrak{D}_0$ geht. Satz (A) ist damit bewiesen.

3. Einen zweiten Beweis für Satz (A) gewinnt man durch Übertragung des l. c.[1]) Nr. 5 erwähnten Beweisverfahrens von *Prüfer*, wie folgt. Nach Voraussetzung ist $\mathfrak{D}_0$ nicht konvex, es gibt also in $\mathfrak{D}_0$ zwei Punkte A, B derart, daß die Strecke AB nicht ganz in $\mathfrak{D}_0$ liegt. Ferner gibt es einen ganz in $\mathfrak{D}_0$ liegenden Streckenzug $AC_1C_2 \ldots C_kB$. Von den Strecken $AC_1, AC_2, \ldots, AC_k, AC_{k+1}$ (wo $B = C_{k+1}$) liegt die erste, AC_1, ganz in $\mathfrak{D}_0$, die letzte, AB, nicht. Sei AC_{h+1} die erste dieser $k+1$ Strecken, die nicht ganz in $\mathfrak{D}_0$ liegt ($1 \leqq h \leqq k$). Ist dann X ein auf der Strecke C_hC_{h+1} von C_h nach C_{h+1} wandernder variabler Punkt, so gibt es für X eine erste Lage X_0 ($= C_{h+1}$ oder zwischen C_h und C_{h+1}) so daß die Strecke AX für diese Lage nicht ganz in $\mathfrak{D}_0$ liegt. Ist dann Z_0 unter den nicht zu $\mathfrak{D}_0$ gehörenden Punkten der Strecke AX_0 der an A nächstgelegene, so ist Z_0 ein Punkt, durch den keine Stützstrecke an $\mathfrak{D}_0$ geht.

4. Beweis der n-dimensionalen Verallgemeinerung von Satz (A)[8]). Sei $\mathfrak{D}_0$ eine zusammenhängende offene nicht-konvexe Menge des $\mathfrak{R}^n$ ($n > 2$). Seien A, B zwei Punkte von $\mathfrak{D}_0$, für welche nicht die ganze Strecke AB in $\mathfrak{D}_0$ liegt und sei $AC_1C_2 \ldots C_kB$ ein in $\mathfrak{D}_0$ liegender Streckenzug. Sei AC_{h+1} unter den Strecken $AC_2, \ldots, AC_k, AC_{k+1}$ (wo $C_{k+1} = B$) die erste nicht ganz in $\mathfrak{D}_0$ liegende. Da die Strecken C_hC_{h+1} und AC_h in $\mathfrak{D}_0$ liegen, AC_{h+1} aber nicht, so können die 3 Punkte A, C_h, C_{h+1} nicht auf einer Geraden liegen. Sie bestimmen also eine zweidimensionale Ebene $\mathfrak{R}^2$. Sei $\mathfrak{D}_*^{(2)}$ der Schnitt von $\mathfrak{D}_0$ mit $\mathfrak{R}^2$. Es ist $\mathfrak{D}_*^{(2)}$ in $\mathfrak{R}^2$ offen und nicht leer. A, C_h, C_{h+1} gehören derselben Komponente (demselben zusammenhängenden Teil) $\mathfrak{D}_0^{(2)}$ von $\mathfrak{D}_*^{(2)}$ an. $\mathfrak{D}_0^{(2)}$ ist dann in der Ebene $\mathfrak{R}^{(2)}$ eine zusammenhängende offene nicht-konvexe Menge (sie ist nicht konvex, weil sie nicht die ganze Strecke AC_{h+1} enthält); nach Satz (A) gibt es also auf der Begrenzung von $\mathfrak{D}_0^{(2)}$ mindestens einen Punkt Z_0, durch den keine Stützstrecke an $\mathfrak{D}_0^{(2)}$ geht. Wir wollen zeigen, daß durch Z_0 keine $(n-1)$-dimensionale Stützscheibe an $\mathfrak{D}_0$ geht.

Es werde mit $\mathfrak{E}$ eine $(n-1)$-dimensionale Ebene durch Z_0 bezeichnet. Wir unterscheiden die Fälle: a) $\mathfrak{E}$ und $\mathfrak{R}^2$ schneiden einander in einer Geraden g; b) $\mathfrak{E}$ enthält ganz die zweidimensionale Ebene $\mathfrak{R}^2$. Im Falle a) gibt es in $\mathfrak{E}$ keine Stützscheibe $\mathfrak{S}$ durch Z_0 an $\mathfrak{D}_0$, weil sonst in $\mathfrak{R}^2$ der Durchschnitt von $\mathfrak{S}$ mit g eine Stützstrecke durch Z_0 an $\mathfrak{D}_0^{(2)}$ wäre, und eine solche Stützstrecke nicht existiert. Im Falle b) gibt es aber ebenfalls in $\mathfrak{E}$ keine Stützscheibe an $\mathfrak{D}_0$, weil in $\mathfrak{R}^2$ und somit in $\mathfrak{E}$ Punkte von $\mathfrak{D}_0^{(2)}$, also Punkte von $\mathfrak{D}_0$ in beliebiger Nähe von Z_0 liegen, woraus folgt, daß in beliebiger Nähe von Z_0 auf beiden Seiten von $\mathfrak{E}$ Punkte von $\mathfrak{D}_0$ liegen.

Somit ist Z_0 tatsächlich ein Punkt, durch den keine Stützscheibe an $\mathfrak{D}_0$ geht.

München, den 9. Januar 1928. (Eingegangen 11. Januar 1928.)

[8]) Vgl. l. c. [1]), Nr. 3.

Über diophantische Gleichungen mit endlich vielen Lösungen[1]).

Von *Alfred Brauer* in Berlin.

Einleitung.

Ist $f(x, y)$ eine ganze rationale Funktion mit ganzen rationalen Koeffizienten, so ist die Frage, wann die diophantische Gleichung $f(x, y) = 0$ unendlich viele ganzzahlige Lösungen haben kann, im allgemeinen noch ungelöst. Solche Gleichungen, bei denen die zugehörige algebraische Kurve das Geschlecht 0 hat, sind von Herrn *D. Hilbert* und *A. Hurwitz*[2]), *H. Poincaré*[3]) und Herrn *E. Maillet*[4]) eingehend behandelt worden. Außerdem konnte man für eine große Anzahl von Klassen diophantischer Gleichungen zeigen, daß sie höchstens endlich viele ganzzahlige Lösungen besitzen können. Insbesondere erhielt *C. Runge*[5]) durch Betrachtung der Potenzreihenentwicklungen der durch die Gleichung $f(x, y) = 0$ definierten algebraischen Funktion von x in der Umgebung von $x = \infty$ mehrere Kriterien dafür, daß die diophantische Gleichung $f(x, y) = 0$ höchstens endlich viele Lösungen in ganzen rationalen Zahlen x, y besitzt[6]). Den eigentlichen Kern der *Runge*schen Untersuchungen bildet der folgende

Satz A: *Ist die Reihe*

$$y = \frac{a_1}{x} + \frac{a_2}{x^2} + \cdots$$

für hinreichend große $|x|$ *konvergent, so nimmt sie höchstens für endlich viele ganze rationale* x *ganze rationale Werte an*[7]).

---

[1]) Die vorliegende Arbeit bildet den ersten Teil meiner Dissertation, die am 12. 7. 1927 der Philosophischen Fakultät der Universität Berlin eingereicht wurde.

[2]) *D. Hilbert* und *A. Hurwitz*. Über die diophantischen Gleichungen vom Geschlecht Null, Acta Mathematica 14 (1890/91) S. 217—224.

[3]) Sur les propriétés arithmétiques des courbes algébriques, Journal de mathématiques pures et appliquées (5) 7 (1901) S. 161—233.

[4]) Détermination des points entiers des courbes algébriques unicursales à coefficients entiers, Comptes rendues de l'Académie des sciences du 27. janvier 1919 und Journal de l'école polytechnique (2) 20 (1919) S. 115—156.

[5]) Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, Journal für die reine und angewandte Mathematik 100 (1887) S. 425—435. Diese Arbeit zitiere ich im folgenden kurz mit *R.*

[6]) Vgl. hierzu auch

a) *Th. Skolem*, Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen, Videnskapsselskapets Skrifter I Mat. Naturw. Klasse 1921, Nr. 17 (zitiert mit *Sk.*).

b) *Th. Skolem*, Über ganzzahlige Lösungen einer Klasse unbestimmter Gleichungen, Norsk Matematisk Forenings Skrifter (1) Nr. 10 (1922) S. 1—12.

c) *K. Dörge*, Über die ganzen rationalen Lösungspaare von algebraischen Gleichungen in zwei Variablen, Inauguraldissertation Berlin 1925, S. 8—15.

d) *Th. Skolem*, Einige Sätze über ganzzahlige Lösungen gewisser Gleichungen, Mathematische Annalen 95 (1925) S. 58—68.

[7]) *R.* S. 425—26 oder *Sk.* S. 10 oder *G. Pólya* und *G. Szegö*, Aufgaben und Lehrsätze aus der Analysis II, Berlin Springer 1925, Abschnitt VIII Aufgabe 188 S. 148 (zitiert mit *P.-Sz.*).

Scheinbar von ganz anderer Natur ist das Kriterium, das *A. Thue*[1]) auf Grund seines Satzes über die Approximation algebraischer Zahlen für diophantische Gleichungen mit höchstens endlich vielen ganzen rationalen Lösungspaaren erhielt. Dieses Resultat wurde dann von Herrn *E. Maillet*[2]) und Herrn *C. Siegel*[3]) verschärft und verallgemeinert. Insbesondere bewies Herr *Siegel* die beiden folgenden Sätze[4]):

Satz B: *Es sei $U(x, y)$ eine binäre Form der Dimension n ohne mehrfache Linearfaktoren mit Koeffizienten aus dem algebraischen Zahlkörper* K, *der vom Grade h in bezug auf den Körper* P *der rationalen Zahlen sei. Man setze*

$$s = \left[\frac{1}{2}\left(\sqrt{4n+1} - 1\right)\right].$$

Ferner sei $V(x, y)$ ein Polynom vom Gesamtgrad v mit Koeffizienten aus K, *welches zu $U(x, y)$ teilerfremd ist. Ist dann*

$$0 \leqq v < n - h\left(\frac{n}{s+1} + s\right),$$

so hat die diophantische Gleichung

$$U(x, y) = V(x, y)$$

nur endlich viele Lösungen in ganzen Zahlen x, y aus K.

Satz C: *Es sei $U(x, y)$ eine binäre Form der Dimension n ohne mehrfache Linearfaktoren mit Koeffizienten aus dem algebraischen Zahlkörper* K, *der vom Grade h in bezug auf den Körper* P *der rationalen Zahlen sei. Man setze*

$$s = \left[\frac{1}{2}\left(\sqrt{4nh+1} - 1\right)\right].$$

Ferner sei $V(x, y)$ ein Polynom vom Gesamtgrad v mit Koeffizienten aus K, *welches zu $U(x, y)$ teilerfremd ist. Es sei h_0 eine ganze positive Zahl. Ist dann*

$$0 \leqq v < n - h_0^{\frac{1}{2}}\left(\frac{nh}{s+1} + s\right),$$

so hat die diophantische Gleichung

$$U(x, y) = V(x, y)$$

höchstens endlich viele Lösungen in ganzen algebraischen Zahlen x, y, deren Grad $\leqq h_0$ ist.

Es sollen im folgenden durch Verbindung der funktionentheoretischen mit der zahlentheoretischen Methode einige Kriterien für binäre diophantische Gleichungen mit höchstens endlich vielen Lösungen aufgestellt werden. In der einfachsten Form lassen sich diese Resultate, ganz roh ausgedrückt, folgendermaßen formulieren:

Es seien p, q, r ganze rationale Zahlen, a_0 eine algebraische Zahl; für hinreichend große $|x|$ sei die Reihe

$$y = a_0 x^{\frac{p}{q}} + \sum_{\nu=r}^{\infty} a_\nu x^{\frac{p-\nu}{q}}$$

konvergent, ferner sei y keine ganze rationale Funktion von $x^{\frac{1}{q}}$. Ist dann r hinreichend groß, d. h. tritt in der Reihe hinter dem ersten Glied eine geeignet große Lücke auf, so wird höchstens für endlich viele ganze rationale x auch y ganz und rational.

---

[1]) Über Annäherungswerte algebraischer Zahlen, Journal für die reine und angewandte Mathematik 135 (1909). S. 284—305.

[2]) Sur un théorème de M. Axel Thue, Nouvelles Annales de Mathématiques (4) 16 (1916) S. 338—345.

[3]) Approximation algebraischer Zahlen, Mathematische Zeitschrift 10 (1921) S. 173—213 (zitiert mit *Sie.*).

[4]) *Sie.* S. 199—201.

Diese Kriterien werden im § 2 bewiesen. Einerseits bilden sie eine Verallgemeinerung des oben genannten *Runge*schen Satzes A, andererseits wird im § 3 gezeigt, daß diese Resultate die *Siegel*schen Sätze B und C als Spezialfälle enthalten, sich aber auch in viel allgemeineren Fällen anwenden lassen. Einige Anwendungen dieser Ergebnisse werde ich in einer demnächst in diesem Journal erscheinenden Arbeit behandeln [1]).

Für den Beweis dieser Kriterien sind einige Sätze über die Approximation algebraischer Zahlen durch algebraische Zahlen erforderlich, die im § 1 bewiesen werden. Den ersten dieser Sätze verdanke ich einer Bemerkung von Herrn *J. Schur*; er ist bisher nicht publiziert worden. Sowohl dieser Satz, wie der auf ganz andere Weise bewiesene Satz 2 ergeben mit verhältnismäßig einfachen Mitteln Resultate über die Approximation algebraischer Zahlen durch algebraische Zahlen. Insbesondere folgt aus Satz 2:

Ist α eine algebraische Zahl n-ten Grades über dem Körper P der rationalen Zahlen, l ein Multiplum von n, so läßt sich eine nur von α und l abhängende Konstante C angeben, derart, daß für alle algebraischen Zahlen ξ vom Grade l, die einem Oberkörper vom Grade $\frac{l}{n}$ über $\mathsf{P}(\alpha)$ angehören, die Ungleichung gilt:

$$|\alpha - \xi| > \frac{C}{H(\xi)},$$

wo $H(\xi)$ die Höhe [2]) von ξ bedeutet.

§ 1. Über die Approximation algebraischer Zahlen durch algebraische Zahlen.

I. Die in der Einleitung erwähnten *Siegel*schen Sätze B und C werden in dieser Arbeit nicht vorausgesetzt werden; dagegen werden die folgenden *Siegel*schen Sätze benutzt:

Satz D [3]): *Es sei ξ eine algebraische Zahl vom Grade $n \geqq 2$ in bezug auf den algebraischen Zahlkörper* K. *Man setze*

$$s = \left[\frac{1}{2}(\sqrt{4n+1} - 1)\right].$$

Dann hat für jedes $\varepsilon > 0$ und jedes $C > 0$ die Ungleichung

$$|\xi - \eta| \leqq \frac{C}{H(\eta)^{\frac{n}{s+1} + s + \varepsilon}}$$

nur endlich viele Lösungen in primitiven Zahlen η aus K, *wo $H(\eta)$ die Höhe von η bedeutet.*

Satz E [3]): *Es sei ξ eine algebraische Zahl vom Grade $n \geqq 2$ in bezug auf den Körper* P *der rationalen Zahlen; h sei eine positive ganze rationale Zahl. Man setze*

$$s = \left[\frac{1}{2}(\sqrt{4n+1} - 1)\right].$$

Dann hat für jedes $\varepsilon > 0$ und jedes $C > 0$ die Ungleichung

$$|\xi - \eta| \leqq \frac{C}{H(\eta)^{h\left(\frac{n}{s+1} + s + \varepsilon\right)}}$$

nur endlich viele Lösungen in algebraischen Zahlen η vom Grade $\leqq h$, wo $H(\eta)$ die Höhe von η bedeutet.

---

[1]) Über diophantische Gleichungen der Form $g^2(x, y) - \mu h^2(x, y) = \gamma y^n$.

[2]) Unter der Höhe $H(\xi)$ einer algebraischen Zahl ξ versteht Herr *Siegel* (*Sie.* S. 178) das Maximum der absoluten Beträge der teilerfremden ganzen rationalen Koeffizienten in der irreduziblen Gleichung, der ξ genügt.

[3]) *Sie.* Satz 1 (S. 178) in Verbindung mit Zusatz 1 und 3 (S. 191) und Hilfssatz X (S. 191).

Wir werden auch von folgenden weit weniger tief liegenden Sätzen Gebrauch machen:

Satz F [1]**:** *Es sei*

$$f(x) = a_0 x^t + a_1 x^{t-1} + \cdots + a_t$$

ein Polynom mit beliebigen Koeffizienten, deren absolute Beträge das Maximum a haben; λ sei eine beliebige Zahl. Man setze

$$g(x) = (x - \lambda) f(x) = c_0 x^{t+1} + c_1 x^t + \cdots + c_{t+1}.$$

Ist dann

$$c = \operatorname{Max}\{|c_0|, |c_1|, \ldots, |c_{t+1}|\},$$

so ist

$$a \leqq c(t+1).$$

Satz G [2]**:** *Ist*

$$s = \left[\frac{1}{2}(\sqrt{4n+1} - 1)\right],$$

so ist

$$2\sqrt{n} - 1 \leqq \frac{n}{s+1} + s \leqq \sqrt{4n+1} - 1.$$

Unter dem Körper P möge in dieser Arbeit immer der Körper der rationalen Zahlen, unter $H(\xi)$ die Höhe der algebraischen Zahl ξ verstanden werden.

II. Es soll zunächst der folgende Satz bewiesen werden, den ich einer Bemerkung von Herrn *Schur* verdanke:

Satz 1: *Ist α eine algebraische Zahl n-ten Grades, h eine ganze rationale Zahl, so gibt es eine nur von α und h abhängende Konstante C, derart daß für alle von α verschiedenen algebraischen Zahlen ξ vom Grade $l \leqq h$ die Ungleichung gilt:*

$$|\alpha - \xi| > \frac{C}{H(\xi)^n}.$$

Beweis: α genüge der irreduziblen Gleichung mit ganzen rationalen teilerfremden Koeffizienten:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

und ξ der irreduziblen Gleichung mit ganzen rationalen teilerfremden Koeffizienten:

$$g(x) = b_0 x^l + b_1 x^{l-1} + \cdots + b_l = 0.$$

Die Konjugierten von α seien $\alpha', \alpha'', \ldots, \alpha^{(n-1)}$, die von ξ seien $\xi', \xi'', \ldots, \xi^{(l-1)}$. Die endlich vielen Fälle, daß ξ eine der Konjugierten von α ist, kann man außer Acht lassen. Dann ist die Resultante R von $f(x)$ und $g(x)$:

$$R = a_0^l g(\alpha)\, g(\alpha') \cdots g(\alpha^{(n-1)}). \tag{1}$$

Nun ist für $\nu = 1, 2, \ldots, n-1$

$$|g(\alpha^{(\nu)})| \leqq H(\xi)\{1 + |\alpha^{(\nu)}| + |\alpha^{(\nu)}|^2 + \cdots + |\alpha^{(\nu)}|^l\} = H(\xi)\, \Gamma_\nu, \tag{2}$$

wo die Konstanten Γ_ν, ebenso wie die im folgenden auftretenden Konstanten Γ^* und Γ, nur von α und l abhängen. Setzt man ferner

$$\varphi(x) = \frac{g(x)}{x - \xi} \tag{3}$$

und bezeichnet man das Maximum der absoluten Beträge der Koeffizienten von $\varphi(x)$ mit M, so ist nach dem Satz F

---

[1]) *Sie.* S. 176.

[2]) *Sie.* S. 191.

$$M \leqq H(\xi)\, l.$$

Folglich ist

$$(4) \qquad |\varphi(\alpha)| \leqq H(\xi) \cdot l\{1 + |\alpha| + |\alpha|^2 + \cdots + |\alpha|^{l-1}\} = H(\xi)\Gamma^*.$$

Nun folgt aus (1) und (3)

$$g(\alpha) = \frac{R}{a_0^l\, g(\alpha')\, g(\alpha'') \cdots g(\alpha^{(n-1)})} = (\alpha - \xi)\ \varphi(\alpha);$$

also ist

$$\alpha - \xi = \frac{R}{a_0^l\ \varphi(\alpha)\ g(\alpha')\ g(\alpha'') \cdots g(\alpha^{(n-1)})}\ .$$

Wegen (2) und (4) ist daher

$$|\alpha - \xi| \geqq \frac{|R|}{|a_0|^l H(\xi)\Gamma^* \cdot H(\xi)^{n-1}\Gamma_1\Gamma_2 \cdots \Gamma_{n-1}} > \frac{|R|}{\Gamma H(\xi)^n}\ .$$

Andererseits ist R eine von 0 verschiedene ganze rationale Zahl, folglich ist

$$|R| \geqq 1\,,$$

$$|\alpha - \xi| > \frac{1}{\Gamma H(\xi)^n}\,.$$

Daher läßt sich eine nur von α und h abhängende Konstante C angeben, derart daß für alle von α verschiedenen algebraischen Zahlen ξ, deren Grad höchstens h ist, die Ungleichung gilt:

$$|\alpha - \xi| > \frac{C}{H(\xi)^n}\ .$$

Die Konstante C läßt sich leicht berechnen.

III. Satz 1 läßt sich auch folgendermaßen formulieren:

Satz 1*: *Ist α eine algebraische Zahl vom Grade n, so gibt es für jedes $C_1 > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele algebraische Zahlen ξ vom Grade $l \leqq h$, für die die Ungleichung gilt*:

$$|\alpha - \xi| \leqq \frac{C_1}{H(\xi)^{n+\varepsilon}}\ .$$

Der Satz 1 sagt aus, daß das bekannte *Liouville*sche Resultat sinngemäß erhalten bleibt, wenn man als approximierende Zahlen nicht nur rationale, sondern algebraische Zahlen von beschränktem Grade nimmt. Im Gegensatz zu den Sätzen D und E gilt Satz 1 auch, wenn α rational ist. Ferner liefert Satz 1 sicher eine bessere Abschätzung als der Satz E, wenn

$$n < h\left(\frac{n}{s+1} + s\right)$$

ist. Nun ist aber nach dem Satz G

$$\frac{n}{s+1} + s \geqq 2\sqrt{n} - 1\,.$$

Satz 1 liefert also jedenfalls eine bessere Abschätzung, wenn

$$n < h(2\sqrt{n} - 1),$$

also

$$h > \frac{n}{2\sqrt{n} - 1}$$

ist.

Durch Verbindung von Satz E und Satz 1* ergibt sich der

Zusatz: *Setzt man*

$$z = \text{Min}\left\{n,\ \ h\left(\frac{n}{s+1} + s\right)\right\},$$

so hat für jedes $C > 0$ *und jedes* $\varepsilon > 0$ *die Ungleichung*

$$|\alpha - \xi| \leqq \frac{C}{H(\xi)^{z+\varepsilon}}$$

höchstens endlich viele Lösungen in algebraischen Zahlen ξ *vom Grade* $\leqq h$.

IV. Satz 1 läßt folgende Verschärfung zu:

Satz 2: *Ist* α *eine ganze algebraische Zahl n-ten Grades in bezug auf den Körper* P *der rationalen Zahlen und* l *eine positive ganze rationale Zahl, so läßt sich eine nur von* α *und* l *abhängende Konstante* C *angeben, derart daß für alle algebraischen Zahlen* $\xi \neq \alpha$ *vom Grade* l *die Ungleichung gilt:*

$$|\alpha - \xi| > \frac{C}{H(\xi)^m},$$

wenn m *den Relativgrad von* α *in bezug auf* $\mathsf{P}(\xi)$ *bezeichnet.*

Beweis: Die endlich vielen Fälle, daß ξ eine der Konjugierten $\alpha', \alpha'', \ldots, \alpha^{(n-1)}$ von α ist, kann man außer Acht lassen. Es seien $\xi', \xi'', \ldots, \xi^{(l-1)}$ die Konjugierten von ξ. Die irreduzible Gleichung mit ganzen rationalen teilerfremden Koeffizienten, der ξ genügt, sei

$$g(x) = b_0 x^l + b_1 x^{l-1} + \cdots + b_l = 0 \qquad (b_0 \geq 1). \tag{5}$$

Es sei m zunächst eine feste positive ganze rationale Zahl $\leqq n$; man betrachte vorläufig nur solche Zahlen ξ vom Grade l, für die α in bezug auf $\mathsf{P}(\xi)$ den Relativgrad m hat. Dann hat der Körper $\mathsf{P}(\alpha, \xi)$ den Grad ml. Man setze

$$ml = t.$$

Faßt man $\alpha - \xi$ als Zahl von $\mathsf{P}(\alpha, \xi)$ auf, so sind die t Konjugierten von $\alpha - \xi$ von der Form

$$\alpha^{(\varkappa)} - \xi^{(\lambda)}; \tag{6}$$

$\varkappa$ durchläuft die Werte $0, 1, \ldots, n-1$; λ die Werte $0, 1, \ldots, l-1$; aber nicht jede Kombination $\varkappa, \lambda$ liefert Konjugierte von $\alpha - \xi$, sondern jedes feste $\xi^{(\lambda)}$ tritt bei der Darstellung der Konjugierten von $\alpha - \xi$ in der Form (6) genau m-mal auf. Die t Konjugierten von $\alpha - \xi$ brauchen nicht sämtlich verschieden zu sein. Es seien $c_1, c_2, \ldots, c_t$ ihre elementarsymmetrischen Funktionen; dann ist jedes c_ν eine ganze rationale Funktion von $\xi, \xi', \ldots, \xi^{(l-1)}$, die in bezug auf jedes $\xi^{(\lambda)}$ höchstens vom Grade m ist. Die Koeffizienten dieser ganzen rationalen Funktion sind wohlbestimmte Zahlen, die unterhalb einer nur von α, l und m abhängenden Schranke liegen. Es sei

$$\Pi = \xi^{(\beta)} \xi^{(\gamma)} \ldots \xi^{(\vartheta)} \tag{7}$$

ein Produkt gewisser voneinander verschiedener der Konjugierten von ξ; die übrigen Konjugierten von ξ seien $\xi^{(\varphi)}, \xi^{(\sigma)}, \ldots, \xi^{(\omega)}$. Dann ist $b_0 \Pi$ das konstante Glied in dem Polynom

$$h(x) = \frac{g(x)}{(x - \xi^{(\varphi)})(x - \xi^{(\sigma)}) \cdots (x - \xi^{(\omega)})}.$$

Also folgt durch mehrmalige Anwendung des Satzes F wegen (5)

$$|b_0 \Pi| < \Gamma^{l-1} H(\xi),$$

wo Γ eine vom Grade l von $g(x)$ abhängige, aber von ξ unabhängige Konstante ist. Andererseits ist jedes c_ν eine Summe, in der jedes Glied ein Produkt von höchstens m gleichen oder verschiedenen Faktoren Π der Form (7) mit beschränkten Koeffizienten ist. Sind $\Pi_1, \Pi_2, \ldots, \Pi_\mu$ solche Faktoren, so ist für $1 \leqq \mu \leqq m$

$$|\Pi_1 \Pi_2 \cdots \Pi_\mu| < \frac{\Gamma^{\mu(l-1)} H(\xi)^\mu}{b_0^\mu} \leqq \frac{\Gamma^{\mu(l-1)} H(\xi)^m}{b_0^m},$$

da nach (5)

$$b_0 \leqq H(\xi)$$

ist. Daher ist für eine geeignete, nur von α, l und m abhängende Konstante Γ_1

$$|c_\nu| < \Gamma_1 \frac{H(\xi)^m}{b_0^m} \qquad (\nu = 1, 2, \ldots, t). \tag{8}$$

Nun genügt $\alpha - \xi$ der Gleichung mit rationalen Koeffizienten:

$$x^t - c_1 x^{t-1} + c_2 x^{t-2} - + \cdots + (-1)^t c_t = 0,$$

also $\dfrac{1}{\alpha - \xi}$ der Gleichung

$$x^t - \frac{c_{t-1}}{c_t} x^{t-1} + \frac{c_{t-2}}{c_t} x^{t-2} - + \cdots + \frac{(-1)^t}{c_t} = 0.$$

Daher ist nach einem bekannten algebraischen Satze

$$\left|\frac{1}{\alpha - \xi}\right| < 1 + \operatorname{Max}\left\{\left|\frac{c_{t-1}}{c_t}\right|, \left|\frac{c_{t-2}}{c_t}\right|, \ldots, \left|\frac{1}{c}\right|\right\}. \tag{9}$$

Andererseits war c_t als Norm von $\alpha - \xi$ ein Produkt von t Zahlen der Form (6). Je m Faktoren enthalten dasselbe $\xi^{(\lambda)}$. Also ist c_t eine ganze rationale Funktion von $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ mit Koeffizienten, die ganze rationale Funktionen von $\xi, \xi', \ldots, \xi^{(l-1)}$ mit ganzen rationalen Zahlenkoeffizienten sind, und zwar sind diese Koeffizienten höchstens vom Grade m in bezug auf jedes $\xi^{(\lambda)}$. Multipliziert man daher c_t mit b_0^m, so wird wegen (5) nach einem bekannten zahlentheoretischen Satze $b_0^m c_t$ eine ganze rationale Funktion von $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ mit ganzen algebraischen Koeffizienten. Nun war α eine ganze algebraische Zahl, also ist auch $b_0^m c_t$ eine ganze algebraische Zahl. Andererseits ist $b_0^m c_t$ eine rationale, folglich eine ganze rationale Zahl. Also ist

$$|b_0^m c_t| \geqq 1,$$

folglich

$$\frac{1}{|c_t|} \leqq b_0^m.$$

Aus (8) folgt daher

$$\left|\frac{c_\nu}{c_t}\right| < \Gamma_1 H(\xi)^m \qquad (\nu = 1, 2, \ldots, t-1).$$

Folglich ist wegen (9)

$$\left|\frac{1}{\alpha - \xi}\right| < 1 + \Gamma_1 H(\xi)^m,$$

$$|\alpha - \xi| > \frac{1}{1 + \Gamma_1 H(\xi)^m} > \frac{C^*}{H(\xi)^m},$$

wo C^* eine nur von α, l und m abhängende Konstante ist.

Da bei festem α für m nur endlich viele Werte in Betracht kommen, gibt es eine nur von α und l abhängende Konstante C, derart daß für alle von α verschiedenen algebraischen Zahlen ξ vom Grade l die Ungleichung gilt:

$$|\alpha - \xi| > \frac{C}{H(\xi)^m}.$$

V. **Zusatz:** *Satz 2 gilt auch für gebrochene algebraische Zahlen* α.

Beweis: Es sei g eine positive ganze rationale Zahl, derart daß $g\alpha$ eine ganze algebraische Zahl ist. Dann läßt sich eine Konstante C_1 angeben, derart daß für alle von $g\alpha$ verschiedenen algebraischen Zahlen ξ vom Grade l die Ungleichung gilt:

$$|g\alpha - \xi| > \frac{C_1}{H(\xi)^m}, \tag{10}$$

wenn m den Relativgrad von α in bezug auf $\mathsf{P}(\xi)$ bedeutet. Es wird nun behauptet, daß für $C = \frac{C_1}{g^{lm+1}}$ und jede von α verschiedene algebraische Zahl η vom Grade l, für die α in bezug auf $\mathsf{P}(\eta)$ vom Grade m ist, die Ungleichung gilt:

$$|\alpha - \eta| > \frac{C}{H(\eta)^m}.$$

Wäre nämlich

$$|\alpha - \eta| \leqq \frac{C_1}{g^{lm+1} H(\eta)^m},$$

so wäre

$$|g\alpha - g\eta| \leqq \frac{C_1}{g^{lm} H(\eta)^m}. \tag{11}$$

Man setze nun

$$\xi = g\eta.$$

Genügt ξ der Gleichung (5), so genügt η der Gleichung

$$b_0 g^l x^l + b_1 g^{l-1} x^{l-1} + \cdots + b_l = 0.$$

Die Koeffizienten dieser Gleichung brauchen nicht teilerfremd zu sein; jedoch ist ihr größter gemeinsamer Teiler

$$d \leqq g^l,$$

da die Koeffizienten von (5) teilerfremd waren. Daher ist

$$H(\xi) \leqq g^l H(\eta).$$

Aus (11) würde also folgen

$$|g\alpha - \xi| \leqq \frac{C_1}{H(\xi)^m}.$$

Dies steht im Widerspruch zu (10).

VI. Während der Satz 1 besagt, daß für die Approximation einer algebraischen Zahl α vom Grade n durch algebraische Zahlen ξ vom Grade l sich eine Konstante C so angeben läßt, daß für alle von α verschiedenen Zahlen ξ die Ungleichung gilt:

$$|\alpha - \xi| > \frac{C}{H(\xi)^n},$$

folgt aus Satz 2, daß sich eine Konstante C_1 so angeben läßt, daß statt des Grades n im Exponenten der jeweilige Relativgrad m von α in bezug auf $\mathsf{P}(\xi)$ genommen werden kann. Daher liefert Satz 2 in vielen Fällen eine bessere Abschätzung als der Satz 1 und demnach oft eine bessere Abschätzung als der *Siegel*sche Satz E.

Aus dem Satz D folgt, daß für jede algebraische Zahl α und beliebige Konstanten $C > 0$ und $\varepsilon > 0$ die Ungleichung

$$|\alpha - \xi| > \frac{C}{H(\xi)^{2+\varepsilon}}$$

für die primitiven Zahlen ξ eines festen Zahlkörpers K gilt, wenn α vom Grade 2 in bezug auf K ist. Aus dem Satz 2 folgt, daß bei geeigneter Wahl von C die schärfere Ungleichung

$$|\alpha - \xi| > \frac{C}{H(\xi)^2}$$

sogar gleichzeitig für die primitiven Zahlen aller Zahlkörper eines festen Grades gilt, für die α vom Relativgrad 2 ist.

VII. Von Interesse ist der folgende Spezialfall des Satzes 2, der schon in der Einleitung erwähnt wurde:

Spezialfall: *Ist α eine algebraische Zahl, l eine positive ganze rationale Zahl, so gibt es eine nur von α und l abhängende Konstante C, derart daß für die primitiven Zahlen ξ aller algebraischen Zahlkörper vom Grade l, die α enthalten, die Ungleichung gilt:*

$$|\alpha - \xi| > \frac{C}{H(\xi)}.$$

Diese Ungleichung gilt erst recht, wenn man für ξ nur primitive Zahlen eines festen Körpers K vom Grade l, der α enthält, zuläßt; d. h. der Satz D gilt auch, wenn α vom Grade 1 in bezug auf K ist, da hier

$$s = \left[\frac{1}{2}(\sqrt{5} - 1)\right] = 0,$$

$$\frac{1}{s+1} + s = 1$$

wird.

VIII. Der Beweis der folgenden drei Sätze soll gemeinsam geführt werden.

Satz 3a: *Es sei q eine positive ganze rationale Zahl, α eine feste algebraische Zahl und zwar sei α^q vom Grade n in bezug auf den algebraischen Zahlkörper K. Man setze*

$$s = \left[\frac{1}{2}(\sqrt{4n+1} - 1)\right],$$

$$z = \frac{n}{s+1} + s.$$

Dann gibt es für jede Konstante $C > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele primitive Zahlen ξ aus K, für die die Ungleichung

$$|\alpha - \sqrt[q]{\xi}| \leqq \frac{C}{H(\xi)^{z+\varepsilon}}$$

erfüllt ist.

Satz 3b: *Es seien q und h positive ganze rationale Zahlen, α eine feste algebraische Zahl und zwar sei α^q vom Grade n in bezug auf den Körper P. Man setze*

$$s = \left[\frac{1}{2}(\sqrt{4n+1} - 1)\right],$$

$$z = \operatorname{Min}\left\{n, h\left(\frac{n}{s+1} + s\right)\right\}.$$

Dann gibt es für jede Konstante $C > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele algebraische Zahlen ξ vom Grade $\leqq h$, für die die Ungleichung gilt:

$$|\alpha - \sqrt[q]{\xi}| \leqq \frac{C}{H(\xi)^{z+\varepsilon}}.$$

Satz 3c: *Es seien q, l und z positive ganze rationale Zahlen, α eine feste algebraische Zahl und zwar sei α^q vom Grade n in bezug auf den Körper* P. *Dann gibt es für jede Konstante $C > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele algebraische Zahlen ξ vom Grade l, für die α^q vom Grade z in bezug auf* P(ξ) *ist und für die die Ungleichung gilt:*

$$|\alpha - \sqrt[q]{\xi}| \leqq \frac{C}{H(\xi)^{z+\varepsilon}}.$$

Beweis: Es genügt, solche Zahlen ξ zu betrachten, für die für mindestens einen der Werte von $\sqrt[q]{\xi}$, der etwa mit ζ bezeichnet werde,

(12) $$|\alpha - \zeta| < 1$$

ist. Es sei ϱ eine primitive q-te Einheitswurzel. Dann ist wegen (12)

(13) $$|\alpha - \varrho^\nu \zeta| \leqq |\alpha| + |\varrho^\nu \zeta| = |\alpha| + |\zeta| \leqq |\alpha| + |\alpha| + 1 = 2|\alpha| + 1 = \Gamma \qquad (\nu = 1, 2, \ldots, q-1),$$

wo Γ eine nur von α abhängende Konstante ist. Nun ist

$$(\alpha - \zeta)(\alpha - \varrho\zeta) \cdots (\alpha - \varrho^{q-1}\zeta) = \alpha^q - \zeta^q = \alpha^q - \xi.$$

Folglich ist nach (13)

(14) $$|\alpha - \zeta| > \frac{|\alpha^q - \xi|}{\Gamma^{q-1}}.$$

Im Fall des Satzes 3a war nun α^q eine algebraische Zahl vom Grade n in bezug auf K, ξ eine den Körper K erzeugende Zahl. Daher folgt für $n \geqq 2$ aus Satz D und für $n = 1$ aus Satz 2 (Spezialfall) für jedes $C' = C\Gamma^{q-1} > 0$ und jedes $\varepsilon > 0$, daß es höchstens endlich viele primitive Zahlen aus K gibt, für die

(15a) $$|\alpha^q - \xi| \leqq \frac{C'}{H(\xi)^{z+\varepsilon}} = \frac{C\Gamma^{q-1}}{H(\xi)^{z+\varepsilon}}$$

ist.

Im Fall des Satzes 3b ist α^q eine algebraische Zahl vom Grade n in bezug auf P. Daher folgt aus Satz 1 (Zusatz), daß für jedes $C' = C\Gamma^{q-1} > 0$ und jedes $\varepsilon > 0$ es höchstens endlich viele algebraische Zahlen ξ vom Grade $\leqq h$ gibt, für die

(15b) $$|\alpha^q - \xi| \leqq \frac{C'}{H(\xi)^{z+\varepsilon}} = \frac{C\Gamma^{q-1}}{H(\xi)^{z+\varepsilon}}$$

ist.

Im Falle des Satzes 3c folgt aus Satz 2 (Zusatz), daß für jedes $C' = C\Gamma^{q-1} > 0$ und jedes $\varepsilon > 0$ es höchstens endlich viele algebraische Zahlen ξ vom Grade l gibt, für die α^q vom Grade z in bezug auf P(ξ) ist und für die die Ungleichung gilt:

(15c) $$|\alpha^q - \xi| \leqq \frac{C'}{H(\xi)^{z+\varepsilon}} = \frac{C\Gamma^{q-1}}{H(\xi)^{z+\varepsilon}}.$$

Aus (14) und (15a) bzw. (15b) bzw. (15c) folgt daher abgesehen von endlich vielen Ausnahmefällen

$$|\alpha - \sqrt[q]{\xi}| = |\alpha - \zeta| > \frac{C}{H(\xi)^{z+\varepsilon}}.$$

IX. Der Satz 3a läßt sich noch etwas erweitern; hierzu braucht man den folgenden

Hilfssatz 1: *Es sei q eine positive ganze rationale Zahl, ξ eine Zahl aus dem algebraischen Zahlkörper* K, *ζ einer der Werte von $\xi^{\frac{1}{q}}$, k die kleinste positive ganze rationale Zahl, für die ζ^k eine Zahl aus* K *ist; ferner enthalte* K *die primitiven k-ten Einheitswurzeln. Dann ist*

$$H(\zeta) = H(\zeta^k).$$

Beweis: Ist ϱ eine primitive k-te Einheitswurzel, so hat die Gleichung

$$x^k - \zeta^k = 0 \tag{16}$$

die Wurzeln $\zeta, \varrho\,\zeta, \varrho^2\,\zeta, \ldots, \varrho^{k-1}\,\zeta$. Wäre nun die Gleichung (16) in K reduzibel, so wäre, wenn $m < k$ der Grad eines der Faktoren wäre, das konstante Glied dieses Faktors von der Form

$$\beta = \varrho^{\nu}\,\zeta^m,$$

wo ν eine ganze rationale Zahl und β eine Zahl aus K ist. Hieraus folgt, da $\varrho < \mathsf{K}$ war,

$$\zeta^m < \mathsf{K}.$$

Dies widerspricht der Voraussetzung, da $m < k$ war. Demnach ist die Gleichung (16) in K irreduzibel.

Man setze nun

$$\zeta^k = \eta_1; \tag{17}$$

die Konjugierten von η_1 seien $\eta_2, \eta_3, \ldots, \eta_t$. Dann genügt η_1 im Körper P der irreduziblen Gleichung

$$(x - \eta_1)\,(x - \eta_2) \cdots (x - \eta_t) = 0. \tag{18}$$

Die Gleichung

$$(x^k - \eta_1)\,(x^k - \eta_2) \cdots (x^k - \eta_t) = 0 \tag{19}$$

hat Koeffizienten aus P; nach (17) ist ζ eine ihrer Wurzeln, ihr Grad ist kt. Wegen der Irreduzibilität von (16) in K ist ζ vom Grade k in bezug auf K, also mindestens vom Grade k in bezug auf $\mathsf{P}(\eta_1)$. Wegen (18) ist η_1 vom Grade t in bezug auf P. Da $\eta_1 < \mathsf{P}(\zeta)$ ist, ist daher ζ in bezug auf P mindestens vom Grade kt, wegen (19) folglich genau vom Grade kt. Daher ist (19) in P irreduzibel. Durch Vergleichen der Koeffizienten von (18) und (19) folgt

$$H(\zeta^k) = H(\zeta).$$

Die Voraussetzungen des Hilfssatzes sind erfüllt, wenn K eine q-te primitive Einheitswurzel enthält. Denn aus der Tatsache, daß k die kleinste positive ganze rationale Zahl war, für die

$$\zeta^k < \mathsf{K},$$

und aus

$$\zeta^q = (\xi^{\frac{1}{q}})^q < \mathsf{K}$$

folgt, daß $k \mid q$ ist.

X. Auf Grund des Hilfssatzes läßt sich nun der Satz 3a folgendermaßen erweitern.

Satz 3a*: *Es sei q eine positive ganze rationale Zahl, α eine feste algebraische Zahl vom Grade n^* in bezug auf den algebraischen Zahlkörper* K. *Die primitiven q-ten Einheitswurzeln seien in* K *enthalten. Man setze*

$$s^* = \left[\frac{1}{2}\left(\sqrt{4\,n^* + 1} - 1\right)\right],$$

$$z^* = \frac{n^*}{s^*+1} + s^*.$$

Dann gibt es für jede Konstante $C > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele primitive Zahlen ξ aus K, *derart daß, wenn ζ einer der Werte von $\xi^{\frac{1}{q}}$ ist, die Ungleichung gilt:*

$$|\alpha - \zeta| \leqq \frac{C}{H(\zeta)^{z^*+\varepsilon}}.$$

Beweis: Es sei k die kleinste positive ganze rationale Zahl, für die $\zeta^k < \mathsf{K}$ ist. Dann ist

$$\mathsf{P}(\zeta^k) < \mathsf{K} = \mathsf{P}(\xi).$$

Andererseits hat, da $k \mid q$ ist, $\zeta^k = \xi^{\frac{k}{q}}$ mindestens denselben Grad wie ξ. Daher ist

$$\mathsf{P}(\zeta^k) = \mathsf{P}(\xi).$$

Es sei ϱ eine primitive k-te Einheitswurzel. Man erhält völlig analog zur Formel (14)

$$|\alpha - \zeta| > \frac{|\alpha^k - \zeta^k|}{\Gamma^{*k-1}}, \tag{20}$$

wo Γ^* eine nur von α abhängende Konstante ist. Nun ist α^k eine algebraische Zahl höchstens vom Grade n^* in bezug auf K, ξ eine den Körper K erzeugende Zahl, also auch ζ^k eine solche. Daher folgt für $n^* \geqq 2$ aus Satz D, für $n^* = 1$ aus Satz 2 (Spezialfall), daß es für jedes $C' = C\Gamma^{*k-1} > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele primitive Zahlen ξ aus K gibt, für die

$$|\alpha^k - \zeta^k| \leqq \frac{C'}{H(\zeta^k)^{z^*+\varepsilon}} \tag{21}$$

ist. Andererseits ist nach Hilfssatz 1

$$H(\zeta^k) = H(\zeta). \tag{22}$$

Daher folgt aus (20), (21) und (22) abgesehen von endlich vielen Ausnahmefällen

$$|\alpha - \zeta| > \frac{C'}{H(\zeta^k)^{z^*+\varepsilon}\,\Gamma^{*k-1}} = \frac{C}{H(\zeta)^{z^*+\varepsilon}}.$$

Satz 3a* kann als eine gewisse Verallgemeinerung des Satzes D aufgefaßt werden, indem als approximierende Zahlen nicht nur primitive Zahlen des Körpers K, sondern für jedes feste positive ganzzahlige q auch alle q-ten Wurzeln aus solchen Zahlen zugelassen werden, vorausgesetzt, daß K die primitiven q-ten Einheitswurzeln enthält.

XI. **Satz 4:** *Es sei q eine positive ganze rationale Zahl, α eine algebraische Zahl und zwar sei α^q vom Grade n in bezug auf den Zahlkörper* K, *der den Grad h in bezug auf* P *habe. Ferner seien ξ und $\eta \neq 0$ ganze Zahlen aus* K; $\xi', \xi'', \ldots, \xi^{(h-1)}$ *und* $\eta', \eta'', \ldots, \eta^{(h-1)}$ *ihre Konjugierten, die untereinander nicht sämtlich verschieden zu sein brauchen, M das Maximum der $2h$ Zahlen* $|\xi|, |\xi'|, \ldots, |\xi^{(h-1)}|, |\eta|, |\eta'|, \ldots, |\eta^{(h-1)}|$. *Man setze*

$$s = \left[\frac{1}{2}\left(\sqrt{4n+1} - 1\right)\right].$$

Dann gibt es für jede Konstante $C > 0$ und jedes $\varepsilon > 0$ höchstens endlich viele Zahlen ξ und η, für die die Ungleichung gilt:

$$\left|\alpha - \sqrt[q]{\frac{\xi}{\eta}}\right| \leqq \frac{C}{M^{h\left(\frac{n}{s+1}+s+\varepsilon\right)}}.$$

Beweis [1]**:** $\frac{\xi}{\eta}$ genügt der Gleichung mit ganzen rationalen Koeffizienten:

$$\varphi(Z) = \prod_{\nu=0}^{h-1} (\eta^{(\nu)} Z - \xi^{(\nu)}) = 0 .$$

Ist

$$\psi(Z) = a_0 Z^d + a_1 Z^{d-1} + \cdots + a_d = 0 \tag{23}$$

die irreduzible Gleichung mit ganzen rationalen teilerfremden Koeffizienten, der $\frac{\xi}{\eta}$ genügt, so gibt es eine ganze rationale Zahl g, derart daß

$$\varphi(Z) = g\{\psi(Z)\}^{\frac{h}{d}}$$

ist. Man kann daher die h Linearfaktoren von $\varphi(Z)$ so in Gruppen zu d Faktoren einteilen, daß das Produkt der d Faktoren jeder Gruppe abgesehen von einer Konstanten gleich $\psi(Z)$ wird. Bei geeigneter Nummerierung der $\xi^{(\nu)}$ und $\eta^{(\nu)}$ ist also

$$\left\{\begin{aligned} &\prod_{\nu=0}^{d-1} (\eta^{(\nu)} Z - \xi^{(\nu)}) = \gamma_1 \psi(Z) , \\ &\prod_{\nu=d}^{2d-1} (\eta^{(\nu)} Z - \xi^{(\nu)}) = \gamma_2 \psi(Z) , \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\prod_{\nu=h-d}^{h-1} (\eta^{(\nu)} Z - \xi^{(\nu)}) = \gamma_{\frac{h}{d}} \psi(Z) , \end{aligned}\right. \tag{24}$$

wo

$$|\gamma_1 \gamma_2 \cdots \gamma_{\frac{h}{d}}| = |g| \geqq 1$$

ist. Daher ist mindestens ein $|\gamma_\lambda|$, etwa

$$|\gamma_1| \geqq 1. \tag{25}$$

Aus (23) und (24) folgt also

$$|\gamma_1 a_\varkappa| < 2^d M^d \qquad (\varkappa = 0, 1, \ldots, d),$$

demnach wegen (25) erst recht

$$|a_\varkappa| < 2^d M^d \qquad (\varkappa = 0, 1, \ldots, d).$$

Daher ist

$$H\left(\frac{\xi}{\eta}\right) < 2^d M^d. \tag{26}$$

Ferner ist $\frac{\xi}{\eta}$ eine primitive Zahl eines Unterkörpers von K. In bezug auf diesen Unterkörper sei α^q vom Grade n'. Dann ist

$$n' \leqq n \frac{h}{d} . \tag{27}$$

Man muß nun 2 Fälle unterscheiden:

1. $n \geqq 2$.

Man setze

$$s' = \left[\frac{1}{2}\left(\sqrt{4n' + 1} - 1\right)\right].$$

[1]) Vgl. hierzu *Sie.* S. 192 Satz 2.

Dann gibt es in jedem der endlich vielen Unterkörper von K für jedes $\varepsilon > 0$ und jedes $C_1 = C \cdot 2^{d\left(\frac{n'}{s'+1}+s'+\varepsilon\right)} > 0$ nach Satz 3 a höchstens endlich viele primitive Zahlen $\frac{\xi}{\eta}$, für die die Ungleichung gilt:

$$\left|\alpha - \sqrt[q]{\frac{\xi}{\eta}}\right| \leqq \frac{C_1}{\left\{H\left(\frac{\xi}{\eta}\right)\right\}^{\frac{n'}{s'+1}+s'+\varepsilon}}.$$

Daher ist abgesehen von endlich vielen Ausnahmefällen für alle Zahlen $\frac{\xi}{\eta}$ aus K wegen (26)

$$(28) \qquad \left|\alpha - \sqrt[q]{\frac{\xi}{\eta}}\right| > \frac{C_1}{\left\{H\left(\frac{\xi}{\eta}\right)\right\}^{\frac{n'}{s'+1}+s'+\varepsilon}} > \frac{C_1}{(2^d M^d)^{\frac{n'}{s'+1}+s'+\varepsilon}} = \frac{C}{M^{d\left(\frac{n'}{s'+1}+s'+\varepsilon\right)}}.$$

Ist $\frac{\xi_0}{\eta_0}$ einer der Ausnahmewerte, ist also

$$(29) \qquad \left|\alpha - \sqrt[q]{\frac{\xi_0}{\eta_0}}\right| \leqq \frac{C}{M^{d\left(\frac{n'}{s'+1}+s'+\varepsilon\right)}},$$

so gibt es nur endlich viele Paare ganzer algebraischer Zahlen ξ_ν, η_ν aus K, für die

$$\sqrt[q]{\frac{\xi_\nu}{\eta_\nu}} = \sqrt[q]{\frac{\xi_0}{\eta_0}}$$

ist und für die die Bedingung (29) erfüllt ist; denn für jedes dieser Zahlenpaare ist

$$\left|\alpha - \sqrt[q]{\frac{\xi_\nu}{\eta_\nu}}\right| = \left|\alpha - \sqrt[q]{\frac{\xi_0}{\eta_0}}\right| = \Gamma,$$

wo Γ eine von ν unabhängige Konstante ist. Andererseits ist

$$d\left(\frac{n'}{s'+1} + s' + \varepsilon\right) > 1.$$

Daher würde aus (29) folgen:

$$(30) \qquad M \leqq \frac{C}{\Gamma}.$$

Da C und Γ Konstanten waren, ist (30) nur für endlich viele ganze algebraische Zahlen ξ_ν, η_ν erfüllt, weil es nur endlich viele ganze algebraische Zahlen gibt, die mit ihren sämtlichen Konjugierten innerhalb eines festen Kreises liegen. Daher gilt die Ungleichung (28) für alle Paare ganzer algebraischer Zahlen ξ, η aus K, abgesehen von endlich vielen Ausnahmefällen.

a) Es sei zunächst

$$\frac{h}{d} \geqq 2;$$

dann ist

$$18\frac{h}{d} - 28\sqrt{\frac{h}{d}} > -5,$$

$$28\left(\frac{h}{d} - \sqrt{\frac{h}{d}}\right) > 10\frac{h}{d} - 5,$$

folglich erst recht

$$20\sqrt{n}\left(\frac{h}{d}-\sqrt{\frac{h}{d}}\right)>10\,\frac{h}{d}-5,$$

$$2\sqrt{n}\left(\frac{h}{d}-\sqrt{\frac{h}{d}}\right)>\frac{h}{d}-\frac{1}{2},$$

$$\frac{h}{d}\,(2\sqrt{n}-1)>2\sqrt{n\,\frac{h}{d}}-\frac{1}{2}. \tag{31}$$

Nun ist nach Satz G

$$\frac{n}{s+1}+s\geqq 2\sqrt{n}-1,$$

folglich wegen (31)

$$h\left(\frac{n}{s+1}+s\right)\geqq d\,\frac{h}{d}\,(2\sqrt{n}-1)>d\left(2\sqrt{\frac{nh}{d}}-\frac{1}{2}\right)>d\left(\sqrt{4\frac{nh}{d}+1}-1\right),$$

da $\frac{nh}{d}>1$ ist.

Daher folgt aus (27) und Satz G

$$h\left(\frac{n}{s+1}+s\right)>d\,(\sqrt{4n'+1}-1)\geqq d\left(\frac{n'}{s'+1}+s'\right). \tag{32}$$

b) Ist dagegen

$$\frac{h}{d}=1,$$

so ist

$$n=n',$$

$$h\left(\frac{n}{s+1}+s\right)=d\left(\frac{n'}{s'+1}+s'\right). \tag{32 a}$$

Also folgt aus (28), (32) und (32 a) für $n\geqq 2$

$$\left|\alpha-\sqrt[q]{\frac{\xi}{\eta}}\right|>\frac{C}{M^{h\left(\frac{n}{s+1}+s+\varepsilon\right)}}. \tag{33}$$

2. $n=1$.

Da als Grad von $\frac{\xi}{\eta}$ nur die endlich vielen Zahlen 1, 2, . . ., h in Betracht kommen, folgt aus Satz 3 c, daß für jedes $\varepsilon>0$ und jedes $C_1=C\cdot 2^{d(n'+\varepsilon)}>0$ es höchstens endlich viele Zahlen $\frac{\xi}{\eta}$ aus K gibt, für die

$$\left|\alpha-\sqrt[q]{\frac{\xi}{\eta}}\right|\leqq\frac{C_1}{\left\{H\left(\frac{\xi}{\eta}\right)\right\}^{n'+\varepsilon}}$$

ist. Analog wie im Fall 1. und aus (26) folgt daher, daß abgesehen von endlich vielen ganzzahligen Wertepaaren ξ, η aus K die Ungleichung gilt:

$$\left|\alpha-\sqrt[q]{\frac{\xi}{\eta}}\right|>\frac{C_1}{(2^d M^d)^{n'+\varepsilon}}=\frac{C}{M^{d(n'+\varepsilon)}}. \tag{34}$$

Aus (27) folgt

$$dn'\leqq hn=h.$$

Daher folgt aus (34), daß auch im Falle $n = 1$ wegen $s = 0$ abgesehen von endlich vielen Ausnahmefällen die Ungleichung gilt:

$$\left| \alpha - \sqrt[q]{\frac{\xi}{\eta}} \right| > \frac{C}{M^{h\left(\frac{n}{s+1}+s+\varepsilon\right)}}.$$

Hieraus und aus (33) erhält man die Behauptung.

§ 2. Kriterien für diophantische Gleichungen mit endlich vielen Lösungen.

XII. Auf Grund der vorhergehenden Sätze sollen nun durch Untersuchung der Potenzreihenentwicklungen der durch die Gleichung $f(x, y) = 0$ definierten algebraischen Funktion von x Kriterien abgeleitet werden, die es ermöglichen, in vielen Fällen die Unmöglichkeit unendlich vieler Lösungen der diophantischen Gleichung $f(x, y) = 0$ zu beweisen. In einigen Fällen braucht man sich nicht auf Potenzreihen zu beschränken, die Zweige einer algebraischen Funktion darstellen, sondern kann allgemeiner untersuchen, ob eine vorgelegte Potenzreihe für unendlich viele ganzzahlige Werte des Arguments ganz sein kann.

Der Satz A läßt sich, etwas allgemeiner als es in der Einleitung getan wurde, folgendermaßen formulieren [1]): Die Reihe

$$y = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 + b_{-1} x^{-1} + \cdots \tag{35}$$

möge außerhalb eines gewissen Kreises konvergieren und stelle keine ganze rationale Funktion von x dar. Sind die Zahlen $b_m, b_{m-1}, \ldots, b_1$ rational, so hat die Gleichung (35) nur endlich viele Lösungen in ganzen rationalen Zahlen x, y.

Dieser Satz läßt folgende Erweiterung zu, bei der der höchste Koeffizient nicht mehr rational, sondern nur algebraisch zu sein braucht. Der höchste auftretende Exponent von x kann von vornherein positiv angenommen werden, da man sonst nur den Satz A erhält.

XIII. **Satz 5:** *Es seien d, d', p, q und r ganze rationale positive Zahlen, p und q seien teilerfremd, a_0 sei eine algebraische Zahl und zwar sei a_0^q eine algebraische Zahl n-ten Grades. Die Reihe*

$$y = a_0 x^{\frac{p}{q}} + a_r x^{\frac{dp-r}{dq}} + \sum_{\nu=1}^{\infty} a_{r+\nu} x^{\frac{d'(dp-r)-\nu}{d'dq}} \tag{36}$$

sei für hinreichend große $|x|$ konvergent. Unter $x^{\frac{1}{d'dq}}$ sei ein fester der $d'dq$ Werte von $\sqrt[d'dq]{x}$ verstanden; es sei $a_r \neq 0$. Man setze

$$s = \left[\frac{1}{2}\left(\sqrt{4n+1} - 1\right)\right],$$

$$z = \frac{n}{s+1} + s.$$

Ist dann

$$r > dpqz, \tag{37}$$

so hat (36) *höchstens endlich viele Lösungen in ganzen rationalen Zahlen x, y.*

Beweis: Es seien x und y ganze rationale Zahlen, die der Gleichung (36) genügen. Aus (36) folgt für hinreichend große $|x|$ und eine geeignete positive Konstante Γ

$$|y - a_0 x^{\frac{p}{q}}| < \Gamma |x|^{\frac{dp-r}{dq}};$$

folglich ist

[1]) *Sk.* oder *P.-Sz.*

$$\left| \frac{y}{x^{\frac{p}{q}}} - a_0 \right| < \Gamma |x|^{\frac{-r}{dq}}.$$

Nur für endlich viele Lösungen von (36) kann

$$\frac{y}{x^{\frac{p}{q}}} - a_0 = 0$$

sein, da

$$a_r x^{\frac{dp-r}{dq}} + \sum_{\nu=1}^{\infty} a_{r+\nu} x^{\frac{d'(dp-r)-\nu}{d'dq}}$$

eine in einer gewissen Umgebung von $x = \infty$ konvergente Potenzreihe ist, also im Innern ihres Konvergenzkreises, abgesehen von einer algebraischen Singularität in $x = \infty$, eine analytische Funktion darstellt und daher dort nur endlich oft verschwinden kann. Diese endlich vielen Lösungspaare lasse man im folgenden außer Acht. Für alle übrigen Lösungen von (36) ist daher

$$0 < \left| \frac{y}{x^{\frac{p}{q}}} - a_0 \right| < \Gamma |x|^{-\frac{r}{dq}}. \tag{38}$$

Ferner folgt aus (36) für hinreichend großes $|x|$ und eine geeignete Konstante $C' > 1$

$$|y^q| < C' |x|^p.$$

Demnach ist, da x und y ganz und rational sind,

$$H\left(\frac{y^q}{x^p}\right) < C' |x|^p. \tag{39}$$

Wegen (37) kann man eine Zahl $\varepsilon_0 > 0$ so wählen, daß

$$r - dpqz > dpq\,\varepsilon_0 > 0 \tag{40}$$

ist. Nun ergibt sich aus Satz 3 a für $\mathsf{K} = \mathsf{P}$, daß für $C = \Gamma C'^{z+\varepsilon_0}$ abgesehen von höchstens endlich vielen Wertepaaren ganzer rationaler Zahlen x, y wegen (39) und (40) die Ungleichung gilt:

$$\left| a_0 - \sqrt[q]{\frac{y^q}{x^p}} \right| > \frac{C}{\left\{H\left(\frac{y^q}{x^p}\right)\right\}^{z+\varepsilon_0}} > \frac{C}{(C'|x|^p)^{z+\varepsilon_0}} = \frac{\Gamma}{|x|^{p(z+\varepsilon_0)}} > \Gamma |x|^{-\frac{r}{dq}},$$

da $|x| > 1$ angenommen werden kann. Dies steht im Widerspruch zur Ungleichung (38). Daher gibt es höchstens endlich viele ganze rationale Lösungspaare x, y von (36).

Bemerkung: Häufig wird Satz 5 erst nach Ausführung einer Substitution anwendbar sein. Insbesondere kann man durch eine Substitution Glieder der Reihe mit nichtnegativen ganzzahligen Exponenten und rationalen Koeffizienten fortschaffen und dadurch die Lücke vergrößern. Ferner kann man einen analogen Satz aufstellen, wenn statt hinter dem ersten Glied der Reihe an einer späteren Stelle der Reihe eine hinreichend große Lücke auftritt. Diese Bemerkung gilt auch für die folgenden Sätze dieses Paragraphen.

XIV. **Hilfssatz 2:** *Es sei $f(x, y)$ eine ganze rationale Funktion von x und y mit Koeffizienten aus dem algebraischen Zahlkörper $\mathsf{P}(\vartheta)$, der den Grad h habe. Eine der Reihenentwicklungen der durch $f(x, y) = 0$ definierten algebraischen Funktion von x in der Umgebung der Stelle $x = \infty$ sei*

$$y = a_0 x^{\frac{p}{q}} + b_0 x^t + \cdots = \mathfrak{P}^{(0)}(x^{\frac{1}{dq}});$$

a_0^q sei eine algebraische Zahl n-ten Grades in bezug auf $\mathsf{P}(\vartheta)$. Drückt man in $f(x, y)$ die Koeffizienten durch ϑ aus und ersetzt ϑ durch eine seiner Konjugierten $\vartheta^{(\lambda)}$, so erhält man eine ganze rationale Funktion $f^{(\lambda)}(x, y)$. Dann hat für $\lambda = 1, 2, \ldots, h-1$ eine der Reihenentwicklungen der durch $f^{(\lambda)}(x, y) = 0$ definierten Funktion von x in der Umgebung der Stelle $x = \infty$ die Form

$$y = a_\lambda x^{\frac{p}{q}} + b_\lambda x^{\cdots} + \cdots,$$

wo a_λ^q vom Grade n in bezug auf $\mathsf{P}(\vartheta^{(\lambda)})$ ist.

Beweis: Nach einem bekannten Satz [1]) gehören die Koeffizienten von $\mathfrak{P}^{(0)}(x^{\frac{1}{dq}})$ sämtlich einem algebraischen Zahlkörper über $\mathsf{P}(\vartheta)$ an; es sei dies der Körper $\mathsf{P}(\zeta)$. Ferner sei $\vartheta = \psi(\zeta)$; die Numerierung der Konjugierten $\zeta^{(\nu)}$ von ζ sei so gewählt, daß für $\lambda = 1, 2, \ldots, h-1$

$$\vartheta^{(\lambda)} = \psi(\zeta^{(\lambda)})$$

ist. Nun ist

$$f\{x, \mathfrak{P}^{(0)}(x^{\frac{1}{dq}})\} = 0. \tag{41}$$

Diese Identität ist gleichbedeutend mit dem Bestehen von unendlich vielen Identitäten, die man aus der Tatsache erhält, daß in (41) die Koeffizienten aller Potenzen von $x^{\frac{1}{dq}}$ verschwinden. Die in ihnen auftretenden Größen sind als Koeffizienten von $f(x, y)$ und $\mathfrak{P}^{(0)}(x^{\frac{1}{dq}})$ sämtlich Zahlen aus $\mathsf{P}(\zeta)$; drückt man sie durch ζ aus und ersetzt ζ durch $\zeta^{(\lambda)}$ für $\lambda = 1, 2, \ldots, h-1$, so bleiben alle Identitäten erhalten, da jede von ihnen nur endlich viele Glieder enthält. Ist daher $\mathfrak{P}^{(\lambda)}(x^{\frac{1}{dq}})$ diejenige Reihe, die man formal erhält, wenn man ζ durch $\zeta^{(\lambda)}$ in den Koeffizienten von $\mathfrak{P}^{(0)}(x^{\frac{1}{dq}})$ ersetzt, so folgt aus (41)

$$f^{(\lambda)}\{x, \mathfrak{P}^{(\lambda)}(x^{\frac{1}{dq}})\} = 0.$$

Also ist

$$y = \mathfrak{P}^{(\lambda)}(x^{\frac{1}{dq}})$$

eine der Reihenentwicklungen der durch $f^{(\lambda)}(x, y) = 0$ definierten Funktion von x in der Umgebung von $x = \infty$. Diese Entwicklung hat die behaupteten Eigenschaften.

XV. Für ganze algebraische Zahlen, die nicht rational sind, gilt der Satz A und die *Runge*schen Resultate über diophantische Gleichungen nicht mehr. Dies zeigt schon das Beispiel

$$y = \frac{1}{x};$$

hier wird, wenn x eine Einheit eines algebraischen Körpers ist, auch y eine solche. Dagegen gilt

Satz 6: *Es sei $f(x, y)$ eine ganze rationale Funktion in x und y mit Koeffizienten aus dem algebraischen Zahlkörper K, dessen Grad h sei. Die Potenzreihenentwicklungen der sämtlichen Zweige der durch $f(x, y) = 0$ definierten algebraischen Funktion von x in der Umgebung der Stelle $x = \infty$ seien*

[1]) Vgl. *R.* S. 430 oder *G. Pólya* und *G. Szegö*, Aufgaben und Lehrsätze aus der Analysis II, Berlin Springer (1925), Abschnitt VIII Aufgabe 235 S. 156.

$$y_\nu = a_{0\nu} x^{\frac{p_\nu}{q_\nu}} + a_{r_{\nu\nu}} x^{\frac{d_\nu p_\nu - r_\nu}{d_\nu q_\nu}} + \sum_{\mu=1}^{\infty} a_{r_\nu+\mu,\nu} x^{\frac{d'_\nu(d_\nu p_\nu - r_\nu)-\mu}{d'_\nu d_\nu q_\nu}} \qquad (\nu = 1, 2, \ldots, N).$$

Für jeden Wert von ν seien p_ν und q_ν teilerfremd, $q_\nu > 0$, $a_{r_{\nu\nu}} \neq 0$; $a_{0\nu}^{q_\nu}$ sei vom Grade n_ν in bezug auf K. *Man setze*

$$(42) \qquad \begin{cases} s_\nu = \left[\frac{1}{2}\left(\sqrt{4n_\nu + 1} - 1\right)\right], \\ z_\nu = \frac{n_\nu}{s_\nu + 1} + s_\nu . \end{cases}$$

Ist dann für $\nu = 1, 2, \ldots, N$ und ein beliebiges $\gamma \geqq 0$

$$(43) \qquad r_\nu > d_\nu h\, q_\nu\, z_\nu\, (|p_\nu| + \gamma),$$

so gibt es unter den Lösungspaaren der diophantischen Gleichung

$$(44) \qquad f(x, y) = 0$$

in ganzen Zahlen x, y aus K *höchstens endlich viele, für die für alle ν*

$$(45) \qquad \begin{cases} \mathrm{Max}\{|y|, |y'|, \ldots, |y^{(h-1)}|\}^{q_\nu} \leqq C \cdot \mathrm{Max}\{|x|, |x'|, \ldots, |x^{(h-1)}|\}^{p_\nu+\gamma} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{für } p_\nu \geqq 0, \\ \mathrm{Max}\{|y|, |y'|, \ldots, |y^{(h-1)}|\}^{q_\nu} \leqq C \cdot \mathrm{Max}\{|x|, |x'|, \ldots, |x^{(h-1)}|\}^{\gamma} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{für } p_\nu < 0 \end{cases}$$

ist, wo $y', y'', \ldots, y^{(h-1)}$ und $x', x'', \ldots, x^{(h-1)}$ die Konjugierten von y und x bedeuten und C eine beliebige feste positive Konstante ist.

Beweis: Angenommen, es gäbe unendlich viele Lösungen der Gleichung (44) in ganzen Zahlen aus K, die außerdem der Bedingung (45) genügen, so betrachte man nur diese Lösungspaare. Ist dann ϑ eine den Körper K erzeugende Zahl, $\vartheta', \vartheta'', \ldots, \vartheta^{(h-1)}$ ihre Konjugierten und

$$x = A(\vartheta), \quad y = B(\vartheta)$$

ein Lösungspaar von (44), das der Bedingung (45) genügt, so ist

$$\left.\begin{aligned} x^{(\lambda)} &= A(\vartheta^{(\lambda)}), \\ y^{(\lambda)} &= B(\vartheta^{(\lambda)}) \end{aligned}\right\} \lambda = 1, 2, \ldots, h-1$$

ein Lösungspaar derjenigen Gleichung, die aus (44) entsteht, wenn man die Koeffizienten durch ϑ ausdrückt und ϑ durch $\vartheta^{(\lambda)}$ ersetzt. Hat daher (44) unendlich viele Lösungen aus K, so hat jede der auf diese Weise aus (44) entstehenden Gleichungen unendlich viele Lösungen aus $\mathsf{P}(\vartheta^{(\lambda)}) = \mathsf{K}^{(\lambda)}$, die der Bedingung (45) genügen. Unter ihnen muß es daher mindestens eine geben, für die unendlich oft der absolute Betrag des zugehörigen $x^{(\lambda)}$ nicht kleiner ist als die absoluten Beträge seiner Konjugierten. Ohne Beschränkung der Allgemeinheit kann man annehmen, daß dies die Gleichung (44) selbst ist, denn die Reihenentwicklungen der konjugierten diophantischen Gleichungen erfüllen nach Hilfssatz 2 in bezug auf den jeweiligen Grundkörper dieselben Voraussetzungen wie die Reihenentwicklungen von (44).

Man betrachte jetzt nur noch die unendlich vielen Lösungspaare x, y aus K von (44), für die die Bedingung (45) erfüllt ist und für die außerdem

$$(46) \qquad |x| = \mathrm{Max}\{|x|, |x'|, \ldots, |x^{(h-1)}|\}$$

gilt. Unter diesen Lösungen muß es ferner unendlich viele solche geben, für die

$$(47) \qquad |x| > C_1$$

ist, wo C_1 eine beliebige positive Konstante ist, über die später noch verfügt werden wird, da es nur endlich viele ganze Zahlen eines algebraischen Zahlkörpers gibt, die mit ihren sämtlichen Konjugierten absolut kleiner als eine feste Konstante sind.

Endlich muß es unter den Zweigen der durch (44) definierten algebraischen Funktion von x mindestens einen geben, der unendlich viele Lösungspaare liefert, die den Bedingungen (45), (46) und (47) genügen.

Unter Abänderung der Bezeichnung sei die Entwicklung dieses Zweiges in der Umgebung des Punktes $x = \infty$

$$y = a_0 x^{\frac{p}{q}} + a_r x^{\frac{dp-r}{dq}} + \sum_{\mu=1}^{\infty} a_{r+\mu} x^{\frac{d'(dp-r)-\mu}{d'dq}} . \tag{48}$$

Es sei a_0^q vom Grade n in bezug auf K; man setze

$$\begin{cases} s = \left[\frac{1}{2}\left(\sqrt{4n+1} - 1\right)\right], \\ z = \frac{n}{s+1} + s. \end{cases} \tag{49}$$

Dann folgt aus (42) und (43)

$$r > dhqz\,(|p| + \gamma). \tag{50}$$

Aus der Annahme, daß (44) unendlich viele ganzzahlige Lösungen aus K besitzt, die der Bedingung (45) genügen, folgt also, daß es auch unendlich viele ganzzahlige Lösungen aus K von (48) gibt, die außerdem den Bedingungen (45), (46) und (47) genügen. Eine Lösung von (48), die diesen Bedingungen genügt, soll kurz eine ausgezeichnete heißen. Es soll nun gezeigt werden, daß höchstens endlich viele ausgezeichnete Lösungen vorhanden sein können.

Es sei also x, y ein ausgezeichnetes Lösungspaar. Die Konstante $C_1 > 1$ sei so groß gewählt, daß aus (48) für $|x| > C_1$ und eine geeignete Konstante Γ analog wie beim Beweise des Satzes 5 die Ungleichung

$$0 < \left| \frac{y}{x^{\frac{p}{q}}} - a_0 \right| < \Gamma\,|x|^{-\frac{r}{dq}} \tag{51}$$

folgt. Nun ist wegen (46)

$$|(x^{(\nu)})^{|p|}| \leqq |x^{|p|}| \qquad (\nu = 1, 2, \ldots, h-1)$$

und wegen (45)

$$\left.\begin{array}{ll} |y^{(\nu)q}| < C\,|x|^{p+\gamma} & \text{für } p \geqq 0 \\ |y^{(\nu)q}| < C\,|x|^{\gamma} & \text{für } p < 0 \end{array}\right\} \quad (\nu = 0, 1, \ldots, h-1;\ y^{(0)} = y).$$

Ist daher M für $p \geqq 0$ das Maximum der $2h$ ganzen Zahlen aus K:

$$x^{(\nu)p},\ y^{(\nu)q} \qquad (\nu = 0, 1, \ldots, h-1;\ x^{(0)} = x)$$

und für $p < 0$ das Maximum der h ganzen Zahlen aus K:

$$(x^{(\nu)})^{-p} \cdot y^{(\nu)q} \qquad (\nu = 0, 1, \ldots, h-1),$$

so ist in beiden Fällen

$$M < C\,|x|^{|p|+\gamma}. \tag{52}$$

Wegen (50) läßt sich eine Zahl $\varepsilon > 0$ angeben, derart daß

$$r > dhq\,(|p| + \gamma)\,(z + \varepsilon) \tag{53}$$

ist. Dann folgt aus Satz 4, daß für $C_2 = \Gamma C^{h(z+\varepsilon)}$ für alle ausgezeichneten Lösungs-

paare x, y von (48), abgesehen von höchstens endlich vielen Ausnahmefällen, wegen (49), (52) und (53) die Ungleichung gilt:

$$\left| \sqrt[q]{\frac{y^q}{x^p}} - a_0 \right| > \frac{C_2}{M^{h(z+\varepsilon)}} > \frac{C_2}{(C\,|x|^{|p|+\gamma})^{h(z+\varepsilon)}} = \frac{\Gamma}{|x|^{h(|p|+\gamma)(z+\varepsilon)}} > \Gamma\,|x|^{-\frac{r}{dq}}.$$

Dies steht im Widerspruch zu (51). Daher hat die Gleichung (44) höchstens endlich viele Lösungen in ganzen Zahlen x, y aus K, für die die Bedingung (45) erfüllt ist.

Bemerkung: Häufig wird es vorteilhaft sein, Reihenentwicklungen einzelner Zweige, in denen das zugehörige $p_\nu < 0$ ist, als Reihen der Form

$$y_\nu = 0 + a_{0\nu}\, x^{\frac{p_\nu}{q_\nu}} + \cdots$$

aufzufassen und die rationale Zahl 0 zu approximieren.

XVI. Satz 6 läßt sich, wie man sofort sieht, auch für Reihen aussprechen, die nicht Reihenentwicklungen algebraischer Funktionen sind. Es gilt:

Zusatz 1: *Es seien d, p, q, r ganze rationale Zahlen, $d > 0$, $q > 0$; p und q seien teilerfremd, a_0 sei eine algebraische Zahl und zwar sei a_0^q vom Grade n in bezug auf den Normalkörper* K, *der den Grad h habe. Die Reihe*

$$y = a_0\, x^{\frac{p}{q}} + a_r\, x^{\frac{dp-r}{dq}} + \cdots \tag{54}$$

sei für hinreichend große $|x|$ konvergent; es sei $a_r \neq 0$. Man setze

$$s = \left[\frac{1}{2}\left(\sqrt{4n+1} - 1\right)\right],$$

$$z = \frac{n}{s+1} + s.$$

Ist dann für ein beliebiges $\gamma \geqq 0$

$$r > hd\,(|p| + \gamma)\,qz,$$

so gibt es unter den Lösungen von (54) *in ganzen Zahlen x, y aus* K *höchstens endlich viele, für die, wenn $x', x'', \ldots, x^{(h-1)}$ und $y', y'', \ldots, y^{(h-1)}$ die Konjugierten von x und y sind, gleichzeitig mit x, y auch $x^{(\lambda)}, y^{(\lambda)}$ $(\lambda = 1, 2, \ldots, h-1)$ eine Lösung von* (54) *ist und für die ferner für eine beliebige feste positive Konstante C die Ungleichung gilt:*

$$\mathrm{Max}\{|y|, |y'|, \ldots, |y^{(h-1)}|\}^q < C \cdot \mathrm{Max}\{|x|, |x'|, \ldots, |x^{(h-1)}|\}^{p+\gamma} \quad \text{für } p \geqq 0,$$

$$\mathrm{Max}\{|y|, |y'|, \ldots, |y^{(h-1)}|\}^q < C \cdot \mathrm{Max}\{|x|, |x'|, \ldots, |x^{(h-1)}|\}^{\gamma} \quad \text{für } p < 0.$$

XVII. **Zusatz 2:** *Die Funktion $f(x, y)$ genüge den im Satz* 6 *gemachten Voraussetzungen, doch mögen ihre Koeffizienten rationale Zahlen sein;* K *sei ein Normalkörper. Ferner sei*

$$\gamma \geqq \mathrm{Max}\left\{\frac{p_\mu q_\nu}{q_\mu} - \frac{p_\nu}{2}(1 + \mathrm{sign}\, p_\nu)\right\} \qquad (\mu, \nu = 1, 2, \ldots, N). \tag{55}$$

Das Maximum der absoluten Beträge der im Endlichen gelegenen singulären Werte von x der durch $f(x, y) = 0$ definierten algebraischen Funktion sei S. Dann hat die diophantische Gleichung $f(x, y) = 0$ entweder nur endlich viele Lösungen in ganzen Zahlen x, y aus K, *oder es liegt im Innern oder auf dem Rande des Kreises mit S um den Nullpunkt der x-Ebene mindestens ein Häufungspunkt von Lösungswerten x.*

Beweis: Die Reihenentwicklungen der durch $f(x, y) = 0$ definierten Funktion von x in der Umgebung des Punktes $x = \infty$:

$$y_\nu = a_{0\nu} x^{\frac{p_\nu}{q_\nu}} + a_{r_\nu \nu}\, x^{\frac{d_\nu p_\nu - r_\nu}{d_\nu q_\nu}} + \sum_{\mu=1}^{\infty} a_{r_\nu+\mu,\nu}\, x^{\frac{d'_\nu(d_\nu p_\nu - r_\nu)-\mu}{d'_\nu d_\nu q_\nu}} \qquad (\nu = 1, 2, \ldots, N)$$

konvergieren außerhalb des Kreises mit S um den Nullpunkt. Hieraus folgt

$$\frac{y_\nu}{x^{\frac{p_\nu}{q_\nu}}} = a_{0\nu} + \mathfrak{P}_\nu \qquad (\nu = 1, 2, \ldots, N),$$

wo $\mathfrak{P}_\nu$ eine gewöhnliche Potenzreihe in $x^{-\frac{1}{d'_\nu d_\nu q_\nu}}$ ist, die außerhalb des Kreises mit dem Radius S konvergiert und also für jedes $\delta > 0$ auf der Peripherie und außerhalb des Kreises mit dem Radius $S + \delta$ um den Nullpunkt beschränkt ist. Daher läßt sich eine Konstante Γ angeben, derart daß für $|x| \geqq S + \delta$

$$(56) \qquad \left.\begin{array}{ll} |y_\nu^{q_\nu}| < \Gamma |x|^{p_\nu} & \text{für } p_\nu \geqq 0 \\ |y_\nu^{q_\nu}| < \Gamma & \text{für } p_\nu < 0 \end{array}\right\} \quad (\nu = 1, 2, \ldots, N)$$

ist. Nun hatte $f(x, y)$ rationale Koeffizienten und K war ein Normalkörper; daher liefern gleichzeitig mit x, y auch ihre Konjugierten $x^{(\lambda)}$, $y^{(\lambda)}$ für $\lambda = 1, 2, \ldots, h-1$ Lösungen von (44) aus K.

Es sei x, y eine solche Lösung, für die

$$(57) \qquad |x^{(\lambda)}| \geqq S + \delta \qquad (\lambda = 0, 1, \ldots, h-1)$$

ist. Ferner sei

$$(58) \qquad \left.\begin{array}{l} |x^{(\varrho)}| = \mathrm{Max}\,\{|x|, |x'|, \ldots, |x^{(\varrho)}|, \ldots, |x^{(h-1)}|\}, \\ |y^{(\sigma)}| = \mathrm{Max}\,\{|y|, |y'|, \ldots, |y^{(\sigma)}|, \ldots, |y^{(h-1)}|\}. \end{array}\right.$$

Dann ist nach einem bekannten Satz $|x^{(\varrho)}| \geqq 1$. Es sei $y^{(\sigma)}$ ein Wert des Zweiges y_σ. Aus (55) folgt

$$\frac{p_\sigma}{q_\sigma} \leqq \frac{\gamma}{q_\nu} + \frac{p_\nu}{2q_\nu}(1 + \mathrm{sign}\, p_\nu) \qquad (\nu = 1, 2, \ldots, N).$$

Daher ist wegen (56) und (58) für $\nu = 1, 2, \ldots, N$

$$(59) \qquad \left\{\begin{array}{ll} |y^{(\sigma)}| < |\Gamma^{\frac{1}{q_\sigma}}|\, |x^{(\sigma)\frac{p_\sigma}{q_\sigma}}| \leqq |\Gamma^{\frac{1}{q_\sigma}}|\, |x^{(\varrho)\frac{p_\sigma}{q_\sigma}}| \leqq |\Gamma^{\frac{1}{q_\sigma}}|\, |x^{(\varrho)\frac{\gamma}{q_\nu}+\frac{p_\nu}{2q_\nu}(1+\mathrm{sign}\,p_\nu)}| & \text{für } p_\sigma \geqq 0, \\ |y^{(\sigma)}| < |\Gamma^{\frac{1}{q_\sigma}}| \leqq |\Gamma^{\frac{1}{q_\sigma}}| \cdot |x^{(\varrho)\frac{\gamma}{q_\nu}+\frac{p_\nu}{2q_\nu}(1+\mathrm{sign}\,p_\nu)}| & \text{für } p_\sigma < 0. \end{array}\right.$$

Setzt man

$$C = \mathrm{Max}\,\{|\Gamma^{\frac{q_1}{q_\sigma}}|, |\Gamma^{\frac{q_2}{q_\sigma}}|, \ldots, |\Gamma^{\frac{q_N}{q_\sigma}}|\},$$

so folgt aus (59) in beiden Fällen

$$\begin{array}{ll} |y^{(\sigma)}|^{q_\nu} < C\, |x^{(\varrho)}|^{\gamma+p_\nu} & \text{für } p_\nu \geqq 0, \\ |y^{(\sigma)}|^{q_\nu} < C\, |x^{(\varrho)}|^{\gamma} & \text{für } p_\nu < 0. \end{array}$$

Dies liefert aber wegen (58) die Bedingung (45). Daher gibt es nach Satz 6 nur endlich viele Lösungen, für die die Bedingung (57) erfüllt ist. Hat also (44) unendlich viele Lösungen in ganzen Zahlen aus K, so muß für jedes Lösungspaar, abgesehen von endlich vielen Ausnahmefällen, mindestens eine der Konjugierten von x innerhalb des Kreises mit dem Radius $S + \delta$ liegen. Da dies für jedes $\delta > 0$ gilt, müssen innerhalb oder auf dem Rande des Kreies mit S um den Nullpunkt unendlich viele Lösungswerte x liegen. Daher liegt im Innern oder auf dem Rande dieses Kreises mindestens ein Häufungspunkt von Lösungswerten x.

Der Zusatz 2 liefert also einen Zusammenhang zwischen den Singularitäten der durch $f(x, y) = 0$ definierten algebraischen Funktion von x und den Lösungen der diophantischen Gleichung $f(x, y) = 0$ in Zahlen aus K. Da mit x, y auch die konjugiert komplexen Zahlen $\bar{x}, \bar{y}$ eine Lösung liefern, weil $f(x, y)$ rationale Koeffizienten hatte, folgt sofort, daß auch im Innern oder auf dem Rande jedes der beiden Halbkreise, in die die reelle Achse den Kreis mit S zerlegt, mindestens ein Häufungspunkt von Lösungswerten x liegen muß. In einigen Spezialfällen kann man statt des Kreises mit S um den Nullpunkt den kleinsten Kreis nehmen, der alle singulären Werte x im Innern oder auf dem Rande enthält. Hierauf soll jedoch nicht näher eingegangen werden.

XVIII. Läßt man als Lösungen der diophantischen Gleichung nicht nur Zahlen eines festen algebraischen Körpers, sondern alle ganzen algebraischen Zahlen von beschränktem Grade zu, so erhält man den folgenden

Satz 7: *Es sei $f(x, y)$ eine ganze rationale Funktion in x und y mit Koeffizienten aus dem algebraischen Zahlkörper* K, *der den Grad h habe. Die Reihenentwicklungen der sämtlichen Zweige der durch $f(x, y) = 0$ definierten Funktion von x in der Umgebung der Stelle $x = \infty$ seien*

$$y_\nu = a_{0\nu} x^{\frac{p_\nu}{q_\nu}} + a_{r_\nu \nu} x^{\frac{d_\nu p_\nu - r_\nu}{d_\nu q_\nu}} + \sum_{\mu=1}^{\infty} a_{r_\nu+\mu,\,\nu} x^{\frac{d'_\nu(d_\nu p_\nu - r_\nu)-\mu}{d'_\nu d_\nu q_\nu}} \qquad (\nu = 1, 2, \ldots, N).$$

Hierbei sei $(p_\nu, q_\nu) = 1$; $q_\nu > 0$, $d_\nu > 0$; $a_{r_\nu} \neq 0$; $a_{0\nu}^{q_\nu}$ sei vom Grade n_ν in bezug auf den Körper P. *Es sei h_0 eine positive ganze rationale Zahl. Man setze*

$$(60) \qquad \begin{cases} s_\nu = \left[\frac{1}{2}\left(\sqrt{4n_\nu + 1} - 1\right)\right], \\ z_\nu = \operatorname{Min}\left\{n_\nu, h_0^2\left(\frac{n_\nu}{s_\nu + 1} + s_\nu\right)\right\}. \end{cases}$$

Ist dann für $\nu = 1, 2, \ldots, N$ und ein beliebiges $\gamma \geqq 0$

$$(61) \qquad r_\nu > d_\nu h_0^2 q_\nu z_\nu (|p_\nu| + \gamma),$$

so hat die diophantische Gleichung

$$(62) \qquad f(x, y) = 0$$

nur endlich viele Lösungen in ganzen algebraischen Zahlen x, y, deren Grade $h_1 \leqq h_0$ bzw. $h_2 \leqq h_0$ in bezug auf P *sind und für die für alle ν die Bedingung gilt:*

$$(63) \qquad \begin{cases} \operatorname{Max}\{|y|, |y'|, \ldots, |y^{(h_2-1)}|\}^{q_\nu} \leqq C \cdot \operatorname{Max}\{|x|, |x'|, \ldots, |x^{(h_1-1)}|\}^{p_\nu+\gamma} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{für } p_\nu \geqq 0, \\ \operatorname{Max}\{|y|, |y'|, \ldots, |y^{(h_2-1)}|\}^{q_\nu} \leqq C \cdot \operatorname{Max}\{|x|, |x'|, \ldots, |x^{(h_1-1)}|\}^{\gamma} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{für } p_\nu < 0, \end{cases}$$

wo $y', y'', \ldots, y^{(h_2-1)}$ und $x', x'', \ldots, x^{(h_1-1)}$ die Konjugierten von y und x bedeuten und C eine beliebige feste positive Konstante ist.

Beweis: Es sei ϑ eine den Körper K erzeugende Zahl, $\vartheta', \vartheta'', \ldots, \vartheta^{(h-1)}$ ihre Konjugierten. Drückt man die Koeffizienten von $f(x, y)$ durch ϑ aus und ersetzt ϑ durch $\vartheta^{(\lambda)}$, so erhält man Polynome, die mit $f^{(\lambda)}(x, y)$ $(\lambda = 0, 1, \ldots, h-1)$ bezeichnet werden mögen. Man setze

$$(64) \qquad F(x, y) = \prod_{\lambda=0}^{h-1} f^{(\lambda)}(x, y).$$

Dann hat $F(x, y)$ rationale Koeffizienten. Nun sei $x_0 = x_0^{(0)}$, $y_0 = y_0^{(0)}$ eine Lösung von (62), $x_0', x_0'', \ldots, x_0^{(h_1-1)}$ bzw. $y_0', y_0'', \ldots, y_0^{(h_2-1)}$ ihre Konjugierten. Die Gleichung in x

$$\prod_{\sigma=0}^{h_2-1} F(x, y_0^{(\sigma)}) = 0$$

hat rationale Koeffizienten und die Wurzel $x = x_0$, also hat sie auch die Wurzeln $x_0', x_0'', \ldots, x_0^{(h_1-1)}$. Daher gibt es zu jedem $x_0^{(\varrho)}$ mindestens ein $y_0^{(\sigma)}$, derart daß $x_0^{(\varrho)}, y_0^{(\sigma)}$ eine Lösung von $F(x, y) = 0$ und daher wegen (64) eine Lösung von (62) oder von einer der konjugierten Gleichungen ist. Hätte nun (62) unendlich viele Lösungen, die der Bedingung (63) genügen, so folgt, analog wie beim Beweise von Satz 6, daß man ohne Beschränkung der Allgemeinheit annehmen könnte, daß mindestens ein Zweig der durch $f(x, y) = 0$ definierten algebraischen Funktion von x unendlich viele ausgezeichnete Lösungen besitzt. Unter Abänderung der Bezeichnung sei die Reihenentwicklung dieses Zweiges in der Umgebung von $x = \infty$

$$y = a_0 x^{\frac{p}{q}} + a_r x^{\frac{dp-r}{dq}} + \sum_{\mu=1}^{\infty} a_{r+\mu} x^{\frac{d'(dp-r)-\mu}{d'dq}}. \tag{65}$$

Es sei a_0^q vom Grade n in bezug auf den Körper P. Man setze

$$\begin{cases} s = \left[\frac{1}{2}\left(\sqrt{4n+1} - 1\right)\right], \\ z = \text{Min}\left\{n, h_0^2\left(\frac{n}{s+1} + s\right)\right\}. \end{cases} \tag{66}$$

Dann folgt aus (60) und (61)

$$r > d h_0^2 q z (|p| + \gamma). \tag{67}$$

Nun sei x, y ein ausgezeichnetes Lösungspaar von (65). Die Konstante $C_1 > 1$ sei so groß gewählt, daß aus (65) für $|x| > C_1$ und für eine geeignete Konstante Γ analog wie beim Beweis des Satzes 5 die Ungleichung

$$0 < \left| \frac{y}{x^{\frac{p}{q}}} - a_0 \right| < \Gamma x^{-\frac{r}{dq}} \tag{68}$$

folgt. Nun genügt $\frac{y^q}{x^p}$ in P der Gleichung

$$\begin{cases} \varphi(Z) = \prod_{\varkappa=0}^{h_1-1} \prod_{\lambda=0}^{h_2-1} \{x^{(\varkappa)p} Z - y^{(\lambda)q}\} = 0 & \text{für } p \geqq 0, \\ \varphi(Z) = \prod_{\varkappa=0}^{h_1-1} \prod_{\lambda=0}^{h_2-1} \{Z - (x^{(\varkappa)})^{|p|} y^{(\lambda)q}\} = 0 & \text{für } p < 0. \end{cases} \tag{69}$$

Da x, y eine ausgezeichnete Lösung war, ist

$$|x^{(\varkappa)}|^{|p|} \leqq |x|^{|p|} \qquad (\varkappa = 1, 2, \ldots, h_1 - 1).$$

Wegen (63) ist

$$\left.\begin{array}{ll} |y^{(\lambda)}|^q < C|x|^{p+\gamma} & \text{für } p \geqq 0 \\ |y^{(\lambda)}|^q < C|x|^{\gamma} & \text{für } p < 0 \end{array}\right\} \quad (\lambda = 0, 1, \ldots, h_2 - 1).$$

In den einzelnen Faktoren von (69) ist daher in beiden Fällen jeder Koeffizient absolut $\leqq C|x|^{|p|+\gamma}$, folglich jeder Koeffizient von $\varphi(Z)$ absolut sicher kleiner als

$$2^{h_1 h_2} C^{h_1 h_2} |x|^{(|p|+\gamma) h_1 h_2} < C_2 |x|^{h_0^2(|p|+\gamma)},$$

wo C_2 eine Konstante ist. Ist nun $\varphi(Z)$ in P irreduzibel, so folgt hieraus

$$H\left(\frac{y^q}{x^p}\right) < C_2 |x|^{h_0^2(|p|+\gamma)}.$$

Ist dagegen $\varphi(Z)$ in P reduzibel,

$$\varphi(Z) = \psi(Z)\,\chi(Z),$$

$\psi(Z) = 0$ die irreduzible Geichung, der $\frac{y^q}{x^p}$ in P genügt, so folgt aus

$$\psi(Z) = \frac{\varphi(Z)}{\chi(Z)}$$

durch mehrmalige Anwendung des Satzes F, daß sich eine Konstante $C_3 > C_2$ angeben läßt, derart daß in allen Fällen

$$H\left(\frac{y^q}{x^p}\right) < C_3 |x|^{h_0^2(|p|+\gamma)} \tag{70}$$

ist. Wegen (67) läßt sich eine Zahl $\varepsilon > 0$ angeben, derart daß

$$r > dh_0^2 q(|p| + \gamma)(z + \varepsilon) \tag{71}$$

ist. Ferner ist $\frac{y^q}{x^p}$ eine algebraische Zahl höchstens vom Grade h_0^2. Daher folgt aus Satz 3 b, daß für $C_4 = \Gamma C_3^{z+\varepsilon}$, abgesehen von höchstens endlich vielen Ausnahmefällen, für die ausgezeichneten Lösungspaare x, y von (62) wegen (66), (70) und (71) die Ungleichung gilt:

$$\left|\sqrt[q]{\frac{y^q}{x^p}} - a_0\right| > \frac{C_4}{\left\{H\left(\frac{y^q}{x^p}\right)\right\}^{z+\varepsilon}} > \frac{\Gamma C_3^{z+\varepsilon}}{\{C_3 |x|^{h_0^2(|p|+\gamma)}\}^{z+\varepsilon}} > \Gamma |x|^{-\frac{r}{dq}}.$$

Dies steht im Widerspruch zu (68). Also gibt es höchstens endlich viele Lösungen von (62), für die die Bedingung (63) erfüllt ist.

Auch hier lassen sich analoge Zusätze wie beim Satz 6 aufstellen.

§ 3. Anwendungen der Kriterien.

XIX. **Hilfssatz 3:** *Es sei $U(x, y)$ eine ganze rationale homogene Funktion der Dimension n ohne mehrfache Linearfaktoren, in der die Koeffizienten von x^n und y^n von 0 verschieden sind. $V_1(x, y), V_2(x, y), \ldots, V_k(x, y)$ seien ganze rationale Funktionen in x und y, deren Gesamtgrade $v_1, v_2, , \ldots, v_k$ seien; die Summe der Glieder von der Dimension v_k in $V_k(x, y)$ sei zu $U(x, y)$ teilerfremd. Ferner sei*

$$\begin{cases} v_\varrho \leqq \dfrac{v_k\,\varrho}{k} & (\varrho = 1, 2, \ldots, k-1), \\ v_k \leqq k(n-1)\ ^1). \end{cases} \tag{72}$$

Man setze

$$t = \frac{-v_k + k(n-1)}{k}. \tag{73}$$

Dann sind die sämtlichen kn Reihenentwicklungen der durch die Gleichung

$$U(x, y)^k + U(x, y)^{k-1} V_1(x, y) + U(x, y)^{k-2} V_2(x, y) + \cdots + U(x, y) V_{k-1}(x, y) + V_k(x, y) = 0 \tag{74}$$

definierten Funktion von x in der Umgebung der Stelle $x = \infty$ von der Form

$$y_\nu = \alpha_\nu x + \beta_\nu x^{-t} + \cdots \qquad (\nu = 1, 2, \ldots, kn);$$

hierbei ist α_ν eine Wurzel der Gleichung

---

[1]) Es genügt, $v_k < kn$ vorauszusetzen; doch wird der Beweis dann ein wenig umständlicher.

$$U(1, y) = 0.$$

Beweis: Es sei

(75) $$U(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n \qquad (a_0 \neq 0,\ a_n \neq 0).$$

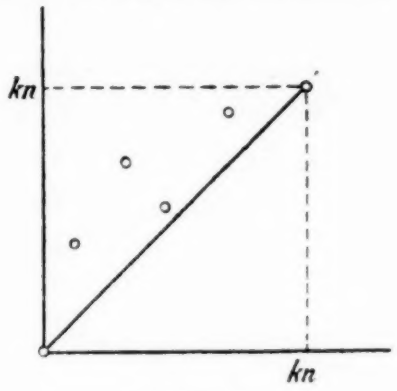
Wegen (72) ist der Gesamtgrad jedes Gliedes in $U(x, y)^{k-\varrho} V_\varrho(x, y)$ für $\varrho = 1, 2, \ldots, k$ kleiner oder gleich

$$(k-\varrho)n + v_\varrho \leqq (k-\varrho)n + \frac{v_k\,\varrho}{k} < (k-\varrho)n + n\varrho = kn.$$

Daher sind in $U(x, y)^{k-\varrho} V_\varrho(x, y)$ alle Glieder von der Form const. $x^\varkappa y^\mu$, wo

$$\varkappa < kn - \mu$$

ist. Dagegen treten in $U(x, y)^k$ die Glieder x^{kn} und y^{kn} auf. Setzt man daher $x = z^{-1}$ und multipliziert (74) mit z^{kn}, so erhält man, abgesehen von den Gliedern von $z^{kn} U(z^{-1}, y)^k$, nur Glieder $z^\lambda y^\mu$, in denen $\lambda > \mu$ ist. Ferner treten in $z^{kn} U(z^{-1}, y)^k$ nur Glieder $z^\mu y^\mu$ auf, das konstante Glied und der Koeffizient von $z^{kn} y^{kn}$ sind hier von 0 verschieden. Daher erhält man das folgende *Puiseux*sche Diagramm:



Figur 1.

da unterhalb der Geraden unter 45^0 durch den Nullpunkt keine der zu markierenden Punkte liegen. Alle Reihenentwicklungen der durch

(76) $$z^{kn}\{U(z^{-1}, y)^k + U(z^{-1}, y)^{k-1} V_1(z^{-1}, y) + \cdots + V_k(z^{-1}, y)\} = 0$$

definierten algebraischen Funktion in der Umgebung der Stelle $z = 0$ sind daher von der Form

(77) $$y_\nu = \alpha_\nu z^{-1} + y_\nu^*.$$

Wegen (75) geht (76) über in

(78) $$\begin{aligned}&(a_0 + a_1 zy + a_2 z^2 y^2 + \cdots + a_n z^n y^n)^k \\ &\qquad + (a_0 + a_1 zy + \cdots + a_n z^n y^n)^{k-1} \cdot z^n V_1(z^{-1}, y) \\ &+ (a_0 + a_1 zy + \cdots + a_n z^n y^n)^{k-2} \cdot z^{2n} V_2(z^{-1}, y) + \cdots + z^{kn} V_k(z^{-1}, y) = 0.\end{aligned}$$

Setzt man hierin (77) ein, so folgt aus dem Obigen, daß nur die folgenden konstanten Glieder auftreten

$$(a_0 + a_1 \alpha_\nu + a_2 \alpha_\nu^2 + \cdots + a_n \alpha_\nu^n)^k.$$

Da diese sich wegheben müssen, ist α_ν eine Wurzel von $U(1, y) = 0$.

Daher folgt aus (78)

(79) $$\begin{aligned}&\Big\{a_1 z y_\nu^* + a_2(2\alpha_\nu z y_\nu^* + z^2 y_\nu^{*2}) + a_3(3\alpha_\nu^2 z y_\nu^* + 3\alpha_\nu z^2 y_\nu^{*2} + z^3 y_\nu^{*3}) \\ &\qquad + \cdots + a_n\Big(\binom{n}{1}\alpha_\nu^{n-1} z y_\nu^* + \binom{n}{2}\alpha_\nu^{n-2} z^2 y_\nu^{*2} + \cdots + \binom{n}{n} z^n y_\nu^{*n}\Big)\Big\}^k \\ &+\Big\{a_1 z y_\nu^* + a_2(2\alpha_\nu z y_\nu^* + z^2 y_\nu^{*2}) + \cdots + a_n\Big(\binom{n}{1}\alpha_\nu^{n-1} z y_\nu^* + \cdots + z^n y_\nu^{*n}\Big)\Big\}^{k-1} \\ &\qquad \cdot z^n V_1(z^{-1}, \alpha_\nu z^{-1} + y_\nu^*) + \cdots + z^{kn} V_k(z^{-1}, \alpha_\nu z^{-1} + y_\nu^*) = 0.\end{aligned}$$

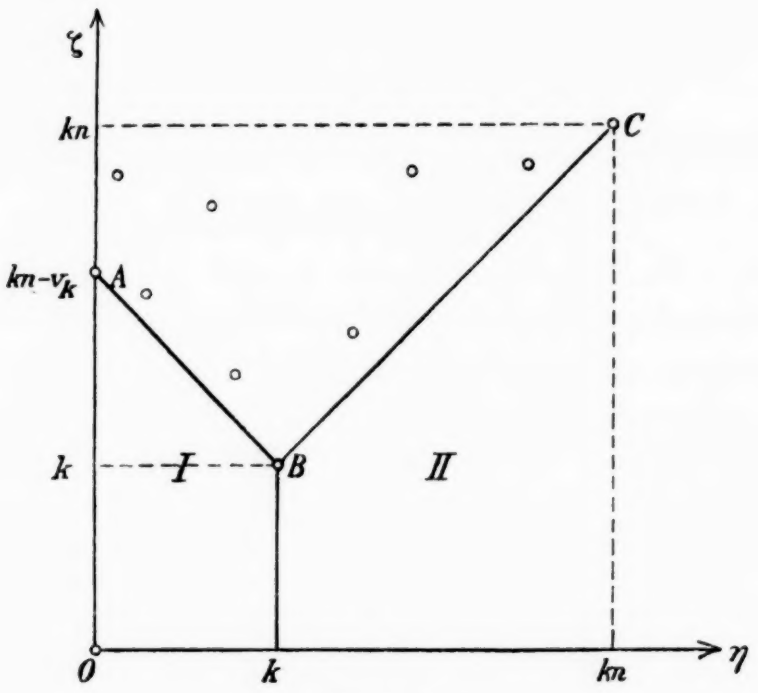
Nur aus der ersten geschweiften Klammer erhält man die Potenz y_ν^{*kn} und zwar mit dem Koeffizienten $a_n^k z^{kn}$. Ferner erhält man aus dieser Klammer $z^k y_\nu^{*k}$ mit dem Koeffizienten

$$(a_1 + 2a_2\alpha_\nu + 3a_3\alpha_\nu^2 + \cdots + na_n\alpha_\nu^{n-1})^k.$$

Dieser Koeffizient ist von 0 verschieden, da sonst $\frac{dU(1,y)}{dy}$ für $y = \alpha_\nu$ verschwinden, also $U(x,y)$ den Linearfaktor $x\alpha_\nu - y$ mindestens doppelt enthalten müßte. In der ersten geschweiften Klammer treten nur Glieder $z^\mu y_\nu^{*\mu}$ auf. Sonst erhält man nur Glieder $z^\lambda y_\nu^{*\mu}$ mit $\lambda > \mu$, so daß jedenfalls die Punkte mit den Koordinaten (k,k) und (kn,kn) Eckpunkte des *Puiseux*schen Diagramms sind. Da $V_k(x,y)$ vom Gesamtgrade v_k war, ist jedes Glied von $z^{kn}V_k\ (z^{-1}, \alpha_\nu z^{-1} + y_\nu^*)$ durch z^{kn-v_k} teilbar; die von y_ν^* freien Glieder, insbesondere die Glieder der Form const. z^{kn-v_k}, können sich hier nicht fortheben, da die Summe $S_k(x,y)$ der Glieder des Grades v_k von $V_k(x,y)$ zu $U(x,y)$ teilerfremd war und daher die Gleichung

$$S_k(1,y) = 0$$

nicht die Wurzel α_ν haben kann. Demnach ist der Punkt mit den Koordinaten $(0, kn - v_k)$ ein Eckpunkt des *Puiseux*schen Diagramms. Man verbinde nun die drei gefundenen Punkte mit den Koordinaten $(0, kn - v_k) = A$, $(k,k) = B$ und $(kn,kn) = C$ durch einen Streckenzug; dann wird behauptet, daß dieser Streckenzug das *Puiseux*sche Diagramm für y_ν^* liefert.



Figur 2.

Aus dem Obigen folgt, daß jedenfalls die Gerade BC (s. Fig. 2) einen Teil des *Puiseux*schen Diagramms bildet. Daher braucht nur noch gezeigt zu werden, daß unterhalb der Geraden AB in dem Trapez I keine der zu markierenden Punkte liegen.

Nun folgt aus (79), daß die aus $z^{kn}U(z^{-1}, \alpha_\nu z^{-1} + y_\nu^*)^k$ hervorgehenden Glieder mindestens durch y_ν^{*k} teilbar sind; die aus $z^{kn}V_k(z^{-1}, \alpha_\nu z^{-1} + y_\nu^*)$ hervorgehenden Glieder waren mindestens durch z^{kn-v_k} teilbar. Alle diese Glieder liefern daher keine Punkte im Innern von I. Alle aus

$$z^{kn}U(z^{-1}, \alpha_\nu z^{-1} + y_\nu^*)^{k-\varrho}V_\varrho(z^{-1}, \alpha_\nu z^{-1} + y_\nu^*)$$

hervorgehenden Glieder sind wegen (79) mindestens durch $y_\nu^{*k-\varrho}\, z^{k-\varrho+\varrho n-v_\varrho}$ teilbar. Tritt unter diesen Gliedern das Glied const. $y_\nu^{*k-\varrho+\sigma}\, z^{k-\varrho+\varrho n-v_\varrho+\tau}$ auf $(\sigma \geqq 0,\ \tau \geqq 0)$, so käme der Punkt mit den Koordinaten $(k-\varrho+\sigma,\ k-\varrho+\varrho n-v_\varrho+\tau)$ als Eckpunkt des Diagramms in Frage. Nun ist die Gleichung der Geraden AB:

$$(\zeta - k)(-k) = (\eta - k)(kn - v_k - k)$$

oder

$$\zeta = \frac{-\eta\,(kn - v_k - k) + k^2 n - k\,v_k}{k} = \eta + (k-\eta)\,n - \frac{v_k\,(k-\eta)}{k}.$$

Daher hat der Schnittpunkt von AB mit der Geraden

$$\eta = k - \varrho$$

die Koordinaten $(k-\varrho,\ k-\varrho+\varrho n - \frac{v_k \varrho}{k})$. Andererseits ist nach (72)

$$k - \varrho + \varrho n - \frac{v_k\,\varrho}{k} \leqq k - \varrho + \varrho n - v_\varrho.$$

Folglich liegt der Punkt mit den Koordinaten $(k-\varrho,\ k-\varrho+\varrho n - v_\varrho)$ nicht unterhalb der Geraden AB, also erst recht der Punkt mit den Koordinaten $(k-\varrho+\sigma,\ k-\varrho+\varrho n - v_\varrho+\tau)$ nicht unterhalb von AB, da nach (72)

$$kn - v_k \geqq k$$

war. Innerhalb des Trapezes I liegen daher keine der zu markierenden Punkte. Folglich bildet auch die Gerade AB einen Teil des *Puiseux*schen Diagramms für y_ν^*. Man erhält also

$$y_\nu^* = \beta_\nu\, z^{\frac{kn-v_k-k}{k}} + \cdots,$$

folglich wegen (77) und (73)

$$y_\nu = \alpha_\nu\, x + \beta_\nu\, x^{\frac{v_k-(n-1)k}{k}} + \cdots = \alpha_\nu\, x + \beta_\nu\, x^{-t} + \cdots.$$

Damit ist der Hilfssatz bewiesen.

Auf Grund dieses Hilfssatzes sollen nun zwei Sätze (8 a und 8 b) gleichzeitig bewiesen werden, die den wesentlichsten Teil der *Siegel*schen Sätze B und C als Spezialfall enthalten und außerdem Resultate liefern, die sich mit der *Siegel*schen Methode nicht ergeben.

XX. **Satz 8:** *Es sei $U(x, y)$ eine binäre Form der Dimension n ohne mehrfache Linearfaktoren mit Koeffizienten aus dem algebraischen Zahlkörper* K, *der in bezug auf* P *vom Grade h sei; $V_1(x, y), V_2(x, y), \ldots, V_k(x, y)$ seien ganze rationale Funktionen in x und y mit Koeffizienten aus* K, *ihre Gesamtgrade seien $v_1, v_2, \ldots, v_k$. Es sei*

$$v_\varrho \leqq \frac{v_k\,\varrho}{k} \qquad (\varrho = 1, 2, \ldots, k-1). \tag{80}$$

Ferner sei die Summe der Glieder der Dimension v_k von $V_k(x, y)$ zu $U(x, y)$ teilerfremd. Man setze

$$\begin{cases} \text{a)} & s = \left[\frac{1}{2}\,(\sqrt{4n+1} - 1)\right], \\ \text{b)} & s' = \left[\frac{1}{2}\,(\sqrt{4nh+1} - 1)\right]. \end{cases} \tag{81}$$

Ist dann, wenn h_0 eine positive ganze rationale Zahl bedeutet,

$$(82)\qquad \begin{cases} \text{a)} & v_k < k\left\{n - h\left(\dfrac{n}{s+1} + s\right)\right\}, \\ \text{b)} & v_k < k\left\{n - h_0^4\left(\dfrac{nh}{s'+1} + s'\right)\right\}, \end{cases}$$

so hat die diophantische Gleichung

$$(83)\quad U(x,y)^k + U(x,y)^{k-1} V_1(x,y) + \cdots + U(x,y) V_{k-1}(x,y) + V_k(x,y) = 0$$

nur endlich viele Lösungen in ganzen Zahlen x, y

a) *aus* K,

b) *von den Graden $h_1 \leqq h_0$ bzw. $h_2 \leqq h_0$.*

Beweis: Durch eine unimodulare Substitution kann man erreichen, daß in (83) die Koeffizienten von x^{kn} und y^{kn} von 0 verschieden sind. Jeder ganzzahligen Lösung der so entstehenden Gleichung entspricht eine ganzzahlige Lösung von (83) und umgekehrt. Daher kann man ohne Beschränkung der Allgemeinheit annehmen, daß in (83) die Koeffizienten von x^{kn} und y^{kn} von 0 verschieden sind. Aus (81) und (82) folgt

$$v_k < k\,(n-1).$$

Folglich sind wegen (80) die Voraussetzungen des Hilfssatzes 3 sämtlich erfüllt. Daher sind alle Reihenentwicklungen der durch (83) definierten algebraischen Funktion von x in der Umgebung der Stelle $x = \infty$ von der Form

$$(84)\qquad y_\nu = \alpha_\nu x + \beta_\nu x^{\frac{-(n-1)k+v_k}{k}} + \cdots,$$

wo α_ν eine Wurzel von $U(1, y) = 0$, also eine algebraische Zahl höchstens vom Grade n in bezug auf den Zahlkörper K ist. Analog sind alle Reihenentwicklungen der durch (83) definierten algebraischen Funktion von y in der Umgebung der Stelle $y = \infty$ von der Form

$$(85)\qquad x_\nu = \alpha'_\nu y + \beta'_\nu y^{\frac{-(n-1)k+v_k}{k}} + \cdots,$$

wo α'_ν eine Wurzel von $U(x, 1) = 0$, also eine algebraische Zahl höchstens vom Grade n in bezug auf K ist.

Es soll nun im Fall a) Satz 6, im Fall b) Satz 7 angewandt werden. In den Bezeichnungen dieser Sätze ist hier für die Reihen (84) und (85)

$$(86)\qquad \left.\begin{cases} N = kn, \\ p_\nu = q_\nu = 1, \\ d_\nu = k \end{cases}\right\} \quad (\nu = 1, 2, \ldots, kn).$$

Ferner ist für die Reihen (84)

$$\left.\begin{aligned} a_{0\nu} &= \alpha_\nu, \\ a_{r_\nu \nu} &= \beta_\nu \end{aligned}\right\} \ (\nu = 1, 2, \ldots, kn)$$

und für die Reihen (85)

$$\left.\begin{aligned} a_{0\nu} &= \alpha'_\nu \\ a_{r_\nu \nu} &= \beta'_\nu \end{aligned}\right\} \ (\nu = 1, 2, \ldots, kn).$$

Nun waren α_ν und α'_ν höchstens vom Grade n in bezug auf K, also höchstens vom Grade nh in bezug auf P. Daher kann man setzen [1])

$$(87)\qquad \left\{\begin{matrix} n_\nu = n & \text{im Fall a),} \\ n_\nu = nh & \text{im Fall b)} \end{matrix}\right\} \ (\nu = 1, 2, \ldots, kn).$$

---

[1]) Ersichtlich gelten die Sätze 6 und 7 erst recht, wenn n_ν nicht der genaue Grad von $a_{0\nu}^{q_\nu}$, sondern eine größere Zahl ist.

Ferner ist wegen (87) und (81)

$$(88)\qquad \left.\begin{cases} s_\nu = s, \\ z_\nu = \dfrac{n}{s+1} + s \end{cases}\right\} \text{im Fall a),} \qquad \left.\begin{cases} s_\nu = s', \\ z_\nu = h_0^2\left(\dfrac{n\,h}{s'+1} + s'\right) \end{cases}\right\} \text{im Fall b)} \qquad (\nu = 1, 2, \ldots, kn).$$

Aus (84) und (85) folgt

$$\frac{d_\nu p_\nu - r_\nu}{d_\nu q_\nu} = \frac{-(n-1)\,k + v_k}{k} \qquad (\nu = 1, 2, \ldots, kn),$$

also wegen (86)

$$r_\nu = nk - v_k.$$

Folglich ist wegen (82), (86) und (88)

$$r_\nu > k\,h\left(\frac{n}{s+1} + s\right) = d_\nu h\, p_\nu q_\nu z_\nu \qquad \text{im Fall a),}$$

$$r_\nu > k\,h_0^4\left(\frac{nh}{s'+1} + s'\right) = d_\nu h_0^2\, p_\nu q_\nu z_\nu \qquad \text{im Fall b).}$$

Daher folgt für $C = 1$ und $\gamma = 0$ wegen (84) aus Satz 6 bzw. aus Satz 7, daß die Gleichung (83) nur endlich viele ganzzahlige Lösungen x, y aus K bzw. von den Graden $h_1 \leqq h_0$ und $h_2 \leqq h_0$ hat, für die

$$(89)\qquad \begin{cases} \text{Max}\,\{|y|, |y'|, \ldots, |y^{(h-1)}|\} \leqq \text{Max}\,\{|x|, |x'|, \ldots, |x^{(h-1)}|\} & \text{im Fall a),} \\ \text{Max}\,\{|y|, |y'|, \ldots, |y^{(h_2-1)}|\} \leqq \text{Max}\,\{|x|, |x'|, \ldots, |x^{(h_1-1)}|\} & \text{im Fall b)} \end{cases}$$

ist. Analog folgt aus (85), daß es nur endlich viele Lösungen gibt, für die

$$(90)\qquad \begin{cases} \text{Max}\,\{|y|, |y'|, \ldots, |y^{(h-1)}|\} \geqq \text{Max}\,\{|x|, |x'|, \ldots, |x^{(h-1)}|\} & \text{im Fall a)} \\ \text{Max}\,\{|y|, |y'|, \ldots, |y^{(h_2-1)}|\} \geqq \text{Max}\,\{|x|, |x'|, \ldots, |x^{(h_1-1)}|\} & \text{im Fall b)} \end{cases}$$

ist. Aus (89) und (90) ergibt sich die Behauptung.

XXI. Der Satz 8 liefert für $k = 1$ im wesentlichen die *Siegel*schen Sätze B und C. Während aber in diesen Sätzen nur vorausgesetzt wird, daß $V_k(x, y)$ zu $U(x, y)$ teilerfremd ist, wurde im Satz 8 die weitergehende Voraussetzung gemacht, daß die Summe der Glieder der höchsten Dimension in $V_k(x, y)$ zu $U(x, y)$ teilerfremd ist. Um zu zeigen, daß die Sätze B und C als Spezialfälle der Sätze 6 und 7 erhalten werden können, kann man einen ähnlichen Satz wie Satz 8 aufstellen, dessen Beweis analog verläuft; man muß nur beim Hilfssatz und bei dem eigentlichen Satz die Voraussetzung hinzunehmen, daß $V_1(x, y)$, $V_2(x, y), \ldots, V_{k-1}(x, y)$ nicht Polynome, sondern Konstanten sind.

Während der Satz 8 eine direkte Anwendung der Kriterien des § 2 darstellt, muß man häufig die gegebenen diophantischen Gleichungen erst auf andere Gleichungen zurückführen, um die Kriterien anwenden zu können. Für eine ziemlich umfangreiche Klasse diophantischer Gleichungen führe ich dies in der am Schluß der Einleitung genannten Arbeit durch.

(Eingegangen 26. März 1928.)

On the differentiability of the integral function.

By *Ganesh Prasad* in Calcutta (India).

Introduction

The question, whether the integral function can be differentiable at a point where the integrand has a discontinuity of the *second* kind, seems to have been considered first about fifty years ago by *Thomae* [1]) and *Dini* [2]) both of whom emphatically answered it in the negative at that time. But, in a paper [3]) published in 1893, *Thomae* pointed out his own and *Dini*'s mistake and gave a criterion for testing the differentiability. *Thomae* gave in that paper some simple examples to show that the integral function may be differentiable; such an example is $\int_0^x \cos\frac{1}{x}\,dx$. *L. Narayan* [4]) seems to have been the next writer to study the question with a view to find types of functions whose integrals are differentiable and his result may be summed up in the statement that $\int_0^x \cos \atop \sin \frac{1}{x^n}\,dx$ is differentiable at the origin whatever positive value n may have. *Narayan*'s result follows immediately from *Thomae*'s criterion.

The object of the present paper is to apply *Paul du Bois-Reymond*'s Infinitärcalcül to obtain as complete an answer to the question as possible.

For the sake of simplicity and fixity of ideas, the point of discontinuity is taken to be $x = 0$ and the integral function is represented as

$$F(x) \equiv \int_0^x f(t)\,dt,$$

the notion of integration being that of *Riemann*. Also throughout the paper $\psi(x)$ denotes a function which is monotone in the neighbourhood of $x = 0$ and which tends to infinity as x tends to zero.

In § 1. I prove that *Thomae*'s criterion gives a sufficient, but not a necessary, condition for the existence of $F'(0)$. In § 2. the case in which $f(t) = \cos\,\psi(t)$ is considered and the necessary *and* sufficient condition is given. § 3. contains a similar condition for the case in which $f(t) = \chi(t)\cos\psi(t)$, χ being limited. In § 4. the case of $f(t) = \chi(t)\cos\psi(t)$ is considered when χ is *not* limited but monotone, and the necessary and sufficient condition is given. In § 5. the cases in which *Thomae*'s criterion fails are considered at length. The paper concludes with the consideration of the case in which $f(t) = \chi(t)\cos\psi(t)$, χ being neither limited nor monotone.

---

[1]) *Einleitung in die Theorie der bestimmten Integrale* (Halle, 1875), p. 17.

[2]) *Fondamenti per la teorica delle funzioni di variabili reali* (Pisa. 1878), pp. 271—272, and p. 318.

[3]) „Über die Differenzierbarkeit eines Integrales nach der oberen Grenze" (*Nachrichten d. Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 1893, pp. 696—700).

[4]) „Integration Images and the failure of the curvature formula" (*Proceedings of the Benares Mathematical Society*, Vols. 4 and 5, 1924).

§ 1. Thomae's criterion gives a sufficient condition.

1. The criterion of *Thomae* is the following: If

$$\lim_{\varepsilon=0} \int_{\varepsilon}^{x} \frac{f(t)}{t}\, dt$$

exists and is finite, then $F'(0)$ exists and is zero.

Proof: —

$$\int_{0}^{x} f(t)\, dt = \lim_{\varepsilon=0} \int_{\varepsilon}^{x} f(t)\, dt.$$

Now

$$\int_{\varepsilon}^{x} f(t)\, dt = \int_{\varepsilon}^{x} t \cdot \frac{f(t)}{t}\, dt$$

$$= \Big[t\, J(t) \Big]_{\varepsilon}^{x} - \int_{\varepsilon}^{x} J(t)\, dt$$

(by integration by parts)

$J(t)$ being a function whose differential coefficient is $\frac{f(t)}{t}$. Thus

$$\text{(A)} \qquad \int_{\varepsilon}^{x} f(t)\, dt = x\, J(x) - \varepsilon\, J(\varepsilon) - \int_{\varepsilon}^{x} J(t)\, dt$$

Therefore, provided that $\varepsilon J(\varepsilon)$ tends to 0 with ε and $J(t)$ is integrable in the interval $(0, x)$, by making ε tend to 0 we deduce from (A) that

$$\text{(B)} \qquad F(x) = x\, J(x) - \int_{0}^{x} J(t)\, dt.$$

Therefore

$$F'(0) = \lim_{x=0} J(x) - \lim_{x=0} \frac{1}{x} \int_{0}^{x} J(t)\, dt.$$

But it follows from the integrability of $\frac{f(t)}{t}$ in the interval $(0,x)$ that $J(x)$ tends to 0 with x. Therefore each limit in the above equation is 0. Therefore $F'(0)$ exists and is zero.

2. The condition that $J(x)$ should tend to 0 with x is *not necessary* for the existence of $F'(0)$.

Proof: —

Consider the case in which

$$J(t) = \cos\left\{\left(\log \frac{1}{t^2}\right)^{\frac{1}{2}}\right\};$$

then, obviously, the condition of *Thomae*'s criterion is not satisfied, for $\lim_{x=0} J(x)$ does not exist.

Now

$$\frac{f(t)}{t} = J'(t) = \frac{1}{t\left(\log \frac{1}{t^2}\right)^{\frac{1}{2}}} \sin\left\{\left(\log \frac{1}{t^2}\right)^{\frac{1}{2}}\right\}.$$

Therefore

$$f(t) = \frac{1}{\left(\log \frac{1}{t^2}\right)^{\frac{1}{2}}} \sin \left\{\left(\log \frac{1}{t^2}\right)^{\frac{1}{2}}\right\}$$

which tends to 0 with t and is, consequently, a continuous function. Hence $F'(0)$ exists and equals 0.

§ 2. Necessary and sufficient condition for the case: $f(t) = \cos \psi(t)$.

3. $F'(0)$ exists or does not exist according as

$$\psi(t) > \log \frac{1}{t^2}$$

or

$$\psi(t) \lesssim \log \frac{1}{t^2}.$$

Proof: —

Consider the three cases separately.

(a) Case: $\psi(t) > \log \frac{1}{t^2}$:

Since

$$\frac{d}{dt}\left(\frac{1}{\psi'} \sin \psi\right) = \cos \psi - \frac{\psi''}{(\psi')^2} \sin \psi,$$

integrating both the sides of the above equality, we have

$$\frac{1}{\psi'(x)} \sin \psi(x) = \int_0^x \cos \psi \, dt - \int_0^x \frac{\psi''}{(\psi')^2} \sin \psi \, dt,$$

i. e.,

$$F(x) \equiv \int_0^x \cos \psi \, dt = \frac{\sin \psi(x)}{\psi'(x)} + \int_0^x \frac{\psi''}{(\psi')^2} \sin \psi \, dt.$$

Now, consider

$$\operatorname*{Lim}_{x=+0} \frac{F(x)}{x}.$$

This equals

$$\operatorname*{Lim}_{x=+0} \frac{\sin \psi(x)}{x \psi'(x)} + \operatorname*{Lim}_{x=+0} \frac{1}{x} \int_0^x \frac{\psi''}{(\psi')^2} \sin \psi \, dt \tag{1}$$

But, since

$$\psi(x) > \log \frac{1}{x},$$

$$\psi'(x) > \frac{1}{x},$$

i. e.

$$x \psi'(x) > 1;$$

also

$$\frac{\psi''}{(\psi')^2} < 1,$$

for

$$\frac{1}{\psi'} < x.$$

Therefore both the limits in (1) exist and equal zero.

Therefore

$$\lim_{x=+0} \frac{F(x)}{x}$$

exists and equals zero.

Similarly it can be proved that

$$\lim_{x=-0} \frac{F(x)}{x}$$

exists and equals zero.

Hence $F'(0)$ exists and equals zero.

4. (b) Case: $\psi(t) < \log \frac{1}{t^2}$.

Integrating by parts,

$$\int_0^x \cos \psi \, dt = x \cos \psi(x) + \int_0^x t \, \psi' \sin \psi \, dt.$$

Now $$\psi(t) < \log \frac{1}{t^2}.$$

Therefore $$\psi' < \frac{1}{t}, \text{ i. e. } t \, \psi' < 1.$$

Therefore $t \, \psi' \sin \psi$ is continuous at $t = 0$ and, consequently,

$$\int_0^x t \, \psi' \sin \psi \, dt$$

has a differential coefficient zero at $x = 0$. Therefore, at $x = 0$, $F(x)$ has no differential coefficient, for

$$x \cos \psi(x)$$

has no differential coefficient at $x = 0$.

5. (c) Case: $\psi(t) \sim \log \frac{1}{t^2}$.

Let $$\psi(t) = \frac{A}{2} \{1 + \sigma(t)\} \log \frac{1}{t^2},$$

where A is a constant and $\sigma < 1$. Then, proceding as in (b), we have

$$\int_0^x \cos \psi(t) \, dt = x \cos \psi(x) + \int_0^x t \, \psi' \sin \psi \, dt$$

$$= x \cos \psi(x) + A \int_0^x \left\{ \frac{1}{2} t \, \sigma' \log \frac{1}{t^2} - (1 + \sigma) \right\} \sin \psi \, dt$$

$$= x \cos \psi(x) - A \int_0^x \sin \psi \, dt + G(x),$$

where G, being the integral function of a continuous integrand which tends to 0 with t, has a differential coefficient zero at $x = 0$.

Therefore, in the limit, we may take

$$\int_0^x \cos \psi \, dt = x \cos \psi(x) - A \int_0^x \sin \psi \, dt.$$

Similarly,

$$\int_0^x \sin\psi\, dt = x \sin\psi(x) + A \int_0^x \cos\psi\, dt.$$

Therefore, as x tends to zero, $F(x)$ behaves as

$$\frac{x\,(\cos\psi - A\sin\psi),}{1 + A^2}$$

i. e. as $$\frac{x}{\sqrt{1+A^2}} \cos(\psi + \operatorname{arctg} A).$$

Hence $F'(0)$ is non-existent.

§ 3. Necessary and sufficient condition for the case $f(t) = \chi(t)\cos\psi(t)$, χ being limited

6. I proceed first to show that this case reduces to the one treated under the preceding head.

For, let

$$\chi(t) = A_1 + \chi_1(t),$$

where A_1 is a constant. Then two possibilities arise:

(I) if χ is monotone, $A_1 \neq 0$ and $\chi_1 < 1$;

(II) if χ is not monotone, χ_1 is of the form $B\cos\psi_1(t)$

where $B \neq 0$ and $\psi_1 > 1$.

Consider the two possibilities separately.

$$\text{(I)} \qquad F(x) \equiv \int_0^x (A_1 + \chi_1)\cos\psi\, dt = A_1 \int_0^x \cos\psi\, dt + \int_0^x \chi_1 \cos\psi\, dt.$$

But $\chi_1 \cos\psi$ is continuous at $t = 0$ and therefore the second integral has a differential coefficient at $x = 0$ equal to 0. Thus

$$F(x) \text{ behaves as } \int_0^x \cos\psi\, dt$$

and the results of § 2 apply.

$$\text{(II)} \qquad F(x) \equiv \int_0^x (A_1 + \chi_1)\cos\psi\, dt = \int_0^x (A_1 + B\cos\psi_1)\cos\psi\, dt$$

$$\text{(2)} \qquad = A_1 \int_0^x \cos\psi\, dt + \frac{B}{2}\int_0^x \cos(\psi + \psi_1)\, dt + \frac{B}{2}\int_0^x \cos(\psi - \psi_1)\, dt$$

Thus in this case too the results of § 2 apply.

7. If $A_1 \neq 0$, $F'(0)$ exists or not according as

$$\psi > \log\frac{1}{t^2} \quad \text{or} \quad \psi \lesssim \log\frac{1}{t^2},$$

ψ_1 not being $\sim \psi$.

Proof: —

(a) Case: $\psi > \log\frac{1}{t^2}$.

By § 2, each of the three integral functions in the equation (2) to whose sum $F(x)$ is equal has a differential coefficient zero at $x = 0$; consequently $F'(0)$ exists and is zero.

(b) Case: $$\psi \lesssim \log \frac{1}{t^2}, \quad \psi_1 > \log \frac{1}{t^2}.$$

By § 2, the second and third integral functions in (2) have each zero as the differential coefficient at $x = 0$, and the first integral function has no differential coefficient at $x = 0$. Hence $F'(0)$ is non-existent.

(c) Case: $$\psi \lesssim \log \frac{1}{t^2}, \quad \psi_1 \lesssim \log \frac{1}{t^2}.$$

There are three possibilities according as

$$\psi < \log \frac{1}{t^2} \text{ and } \psi_1 < \log \frac{1}{t^2},$$

$$\psi < \log \frac{1}{t^2} \text{ and } \psi_1 \sim \log \frac{1}{t^2},$$

or $$\psi \sim \log \frac{1}{t^2} \text{ and } \psi_1 < \log \frac{1}{t^2}.$$

It is easily seen from (2) and § 2 that, in every one of the above three cases, $F'(0)$ is non-existent.

8. Let $\psi_1 \sim \psi$. Then $F'(0)$ is non-existent when

$$\psi \lesssim \log \frac{1}{t^2};$$

and, when

$$\psi > \log \frac{1}{t^2},$$

$F'(0)$ exists or not according as

$$\psi - \psi_1 > \log \frac{1}{t^2} \quad \text{or} \quad \psi - \psi_1 \lesssim \log \frac{1}{t^2},$$

provided that it is understood that $F'(0)$ always exists if

$$\psi - \psi_1 \sim 1.$$

The above theorem is easily seen to follow from (2) and § 2.

If $A_1 = 0$, the result of the preceding paragraph is affected only to this extent that, in the case considered under (b), $F'(0)$ exists.

§ 4. Case: $f(t) = \chi(t) \cos \psi(t)$, χ being unlimited and monotone

9. $F'(0)$ exists or not according as

$$\frac{\chi}{\psi'} < t \text{ or } \frac{\chi}{\psi'} \gtrsim t.$$

Proof: —

Consider separately the various cases that arise.

(a) Case: $$\frac{\chi}{\psi'} < t.$$

$$F(x) \equiv \int_0^x \chi(t) \cos \psi(t)\, dt = \int_0^x \frac{\chi}{\psi'} \cdot \psi' \cos \psi \, dt$$

$$= \left[\frac{\chi}{\psi'} \sin \psi\right]_0^x - \int_0^x \frac{d}{dt}\left(\frac{\chi}{\psi'}\right) \sin \psi \, dt$$

(by integration by parts).

Now, as was proved by *Du Bois Reymond*, the integrability of $\chi \cos \psi$ necessitates that

$$\frac{\chi}{\psi'} < 1.$$

Therefore

(3). $$F(x) = \frac{\chi(x)}{\psi'(x)} \sin \psi(x) - \int_0^x \frac{d}{dt}\left(\frac{\chi}{\psi'}\right) \sin \psi \, dt$$

But $$\frac{\chi}{\psi'} < t,$$

therefore $$\frac{d}{dt}\left(\frac{\chi}{\psi'}\right) < 1.$$

Therefore each of the two terms in (3) whose sum is $F(x)$ has a differential coefficient equal to zero at $x = 0$. Therefore $F'(0) = 0$.

10. (b) Case: $$\frac{\chi}{\psi'} \sim t.$$

Since $$\frac{d}{dt}\left(\frac{\chi}{\psi'}\right) \sim 1,$$

the integral in (3) behaves as

$$\int_0^x \sin \psi \, dt.$$

But, by supposition,

$$\psi' \sim \frac{\chi}{t} > \frac{1}{t}.$$

Therefore

$$\psi > \log \frac{1}{t^2}.$$

Therefore, by § 2,

$$\int_0^x \sin \psi \, dt$$

has zero as its differential coefficient at $x =$ ó. Again the integrated part in (3) is

$$\frac{\chi(x)}{\psi'(x)} \sin \psi(x)$$

which behaves as

$$x \sin \psi(x)$$

and has, consequently, no differential coefficient at $x = 0$. Therefore $F'(0)$ is non-existent.

11. (c) Case: $\dfrac{\chi}{\psi'} > t, \quad \psi > \log \dfrac{1}{t^2}$.

By repeated integration by parts, we have

$$F(x) \equiv \int_0^x \chi(t) \cos \psi(t)\, dt$$

$$= \frac{\chi}{\psi'} \sin \psi + \frac{1}{\psi'} \frac{d}{dx}\left(\frac{\chi}{\psi'}\right) \cos \psi$$

$$- \frac{1}{\psi'} \left\{\frac{d}{dx}\left(\frac{1}{\psi'} \frac{d}{dx} \frac{\chi}{\psi'}\right)\right\} \sin \psi - \frac{1}{\psi'} \left[\frac{d}{dx}\left\{\frac{1}{\psi'} \frac{d}{dx}\left(\frac{1}{\psi'} \frac{d}{dx} \frac{\chi}{\psi'}\right)\right\}\right] \cos \psi$$

$$+ \cdots$$

Now in each term in the above the coefficient of the sine or cosine is infinitarily less than the preceding coefficient. For, consider the first two coefficients, viz.

$$\frac{\chi}{\psi'} \text{ and } \frac{1}{\psi'} \frac{d}{dx} \frac{\chi}{\psi'} .$$

Then, by supposition,

$$\frac{\chi}{\psi'} > x .$$

Therefore

$$\frac{1}{\dfrac{\chi}{\psi'}} < \frac{1}{x} ,$$

i. e.

$$\log \frac{1}{\dfrac{\chi}{\psi'}} < \log \frac{1}{x^2} < \psi .$$

Therefore

$$\frac{\dfrac{d}{dx}\left(\dfrac{\chi}{\psi'}\right)}{\dfrac{\chi}{\psi'}} < \psi'$$

i. e.

$$\frac{1}{\psi'} \frac{d}{dx}\left(\frac{\chi}{\psi'}\right) < \frac{\chi}{\psi'} .$$

Similarly for the other coefficients.

Therefore $F(x)$ behaves as

$$\frac{\chi(x)}{\psi'(x)} \sin \psi'(x) ,$$

and, consequently, $F'(0)$ is non-existent.

12. (d) Case: $\dfrac{\chi}{\psi'} > t, \quad \psi \sim \log \dfrac{1}{t^2}$.

Since, because of the integrability of $\chi \cos \psi$,

$$\frac{\chi}{\psi'} < 1 ,$$

we have

$$\chi < \frac{1}{t} .$$

Let therefore,

$$\chi = \frac{1}{t}\,\theta(t) \quad \text{where} \quad \theta < 1.$$

Then

$$\int_0^x \chi \cos\psi\, dt = \int_0^x \theta \cdot \frac{1}{t} \cos\psi\, dt \sim \int_0^x \theta \cdot \frac{1}{t} \cos \log \frac{1}{t}\, dt.$$

But the last integral equals

$$-\theta \sin \log \frac{1}{t} + \int_0^x \theta' \sin \log \frac{1}{t}\, dt.$$

Two possibilities arise: either $\frac{\theta'}{\theta} \sim \frac{1}{t}$ or $\frac{\theta'}{\theta} < \frac{1}{t}$. It can be easily proved that in the first event the integral behaves as

$$\theta(x) \sin \left\{ \log \frac{1}{x} + \text{constant} \right\}$$

and in the second as

$$-\theta(x) \sin \log \frac{1}{x}.$$

Therefore, in either event, $F'(0)$ is non-existent.

13. (e) Case: $\qquad \frac{\chi}{\psi'} > t, \quad \psi < \log \frac{1}{t^2}.$

By repeated integration by parts, we have

$$F(x) \equiv \int_0^x \chi \cos\psi\, dt = (S \cos\psi + S_1 \sin\psi) - (S_2 \cos\psi + S_3 \sin\psi) + \cdots$$

where

$$S = \int_0^x \chi\, dt, \quad S_1 = \int_0^x \psi' S\, dt, \quad S_2 = \int_0^x \psi' S_1\, dt, \quad \text{etc.}$$

Now it is easily seen that

$$\frac{d}{dx}\left(\frac{\chi}{\psi'}\right) > \chi.$$

Therefore

$$\frac{\chi}{\psi'} > S;$$

hence

$$S > S_1, \quad S_1 > S_2 > S_3 \ldots.$$

Thus it is proved that $F(x)$ behaves as $S \cos\psi$. But

$$S > t,$$

consequently $F'(0)$ is non-existent.

§ 5. Failure of Thomae's Criterion.

14. We are now in a position to prove the following: Of all those cases in which $J(t)$ is of the form

$$\chi(t) \cos\psi(t),$$

where χ is either limited, or unlimited and monotone, the only ones in which $F'(0)$ can exist are those for which

$$\psi < \log \frac{1}{t^2}$$

and either

$$\text{(I) } \chi = \text{constant or behaves as a constant,}$$

$$\text{or (II) } \chi > 1, \quad \frac{\chi}{\psi'} > t.$$

Proof: —

Consider separately the various possibilities.

(a) Let $$J(t) = \cos \psi(t).$$

Then $$f(t) = t\, J'(t) = -\, t\, \psi' \sin \psi.$$

(I) Therefore if

$$\psi < \log \frac{1}{t^2},$$

$$\psi' < \frac{1}{t}$$

i. e. $$t\, \psi' < 1;$$

consequently $f(t)$ is a continuous function at $t = 0$. Therefore $F'(0)$ is existent and zero

(II) If $$\psi \gtrsim \log \frac{1}{t^2},$$

it follows from § 2 that: $F(x)$, which, according to (B) of § 1, equals

$$x\, J(x) - \int_0^x J(t)\, dt,$$

behaves as

$$x \cos \psi(x) \text{ when } \psi > \log \frac{1}{x^2}$$

and as

$$x \cos (\psi + \text{constant}) \text{ when } \psi \sim \log \frac{1}{x^2}.$$

In either case, $F'(0)$ is non-existent.

(b) When

$$J(t) = \chi(t) \cos \psi(t)$$

and χ is limited but not monotone, § 3 shows that $F'(0)$ does not exist.

(c) When

$$J(t) = \chi(t) \cos \psi(t)$$

and χ is unlimited but monotone, the consideration of the various types discussed in § 4 shows (I) that $F'(0)$ *can* exist only when $\psi < \log \frac{1}{t^2}$ and $\frac{\chi}{\psi'} > t$, and (II) that $F'(0)$ certainly exists if

$$\chi\, t\, \psi' < 1.$$

§ 6. Case: $f(t) = \chi(t) \cos \psi(t)$, χ being neither limited nor monotone.

15. Let

$$\chi(t) = \chi_0(t) + \chi_1(t) \cos \psi_1(t),$$

where both χ_0 and χ_1 are monotone and $\psi_1 > 1$. Then

$$F(x) \equiv \int_0^x \chi \cos \psi \, dt = \int_0^x (\chi_0 + \chi_1 \cos \psi_1) \cos \psi \, dt$$

$$= \int_0^x \chi_0 \, dt + \frac{1}{2} \int_0^x \chi_1 \cos (\psi + \psi_1) \, dt + \frac{1}{2} \int_0^x \chi_1 \cos (\psi - \psi_1) \, dt,$$

and therefore the question of the existence of $F'(0)$ can be completely settled by using the results of § 2 and § 4. A large number of possibilities present themselves according to the behaviour of χ_0, χ_1, ψ and ψ_1 as t tends to zero. It is not necessary to give in detail the various results; the following results will suffice: —

(a) If $\chi_0 \gtrsim \chi_1$ and $\psi < \psi_1$, then $F'(0)$ exists when

$$\frac{\chi_0}{\psi'} < t.$$

(b) $F'(0)$ is non-existent, if at least one of the three relations holds:

$$\frac{\chi_0}{\psi'} \gtrsim t, \quad \frac{\chi_1}{\psi_1' + \psi'} \gtrsim t, \quad \frac{\chi_1}{\psi_1' - \psi'} \gtrsim t.$$

Eingegangen am 2. Oktober 1927.

Distributive Gruppen von endlicher Ordnung.

Von *C. Burstin* in Wien und *W. Mayer* in Wien.

§ 1. Die Axiomatik distributiver Gruppen.

Es sei ein System von endlich oder unendlich vielen Elementen gegeben:

$$a, b, c, \ldots$$

und eine Verknüpfung, die je zwei Elementen a, b in der bestimmten Reihenfolge a, b ein Element $a \,.\, b$, das Verknüpfungsresultat von a und b zuordnet. Sind dann die folgenden drei Axiome erfüllt, so wollen wir ein solches System eine *distributive Gruppe* nennen.

I. Axiom: Das Verknüpfungsresultat $a \,.\, b$ irgend zweier Elemente a und b des Systems ist ein Element des Systems.

II. Axiom: Seien a und b irgend zwei Elemente des Systems, so haben die beiden Gleichungen

$$a \,.\, x = b \quad \text{resp.} \quad y \,.\, a = b$$

im System je eine und nur eine Lösung.

(Dieses Axiom verlangt somit die Existenz und die Eindeutigkeit der inversen Operationen.)

III. Axiom: Seien a, b und c irgend drei Elemente des Systems, so bestehen identisch die beiden Relationen

$$(a \,.\, b) \,.\, c = (a \,.\, c) \,.\, (b \,.\, c), \qquad c \,.\, (a \,.\, b) = (c \,.\, a) \,.\, (c \,.\, b)$$

Die Axiome I und II sind Axiome der klassischen Gruppentheorie, an Stelle des dritten Axioms tritt dort das Axiom der assoziativen Verknüpfung: $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$, wir werden daher die Gruppen der klassischen Theorie zur Unterscheidung von den distributiven Gruppen *assoziative* Gruppen nennen.

Liegt ein Axiomensystem vor, so sind vor allem die Fragen nach der Unabhängigkeit und nach der Widerspruchslosigkeit der Axiome zu beantworten.

Wir zeigen an einem Beispiele die Unabhängigkeit des Axioms I von den Axiomen II und III:

Das System der Elemente seien die (positiven und negativen) *ganzen* Zahlen; für die Verknüpfung gelte $a \,.\, b = \dfrac{a + b}{2}$. Hier sind Axiom II und III erfüllt, dagegen nicht Axiom I.

Im Systeme *von endlich vielen* Elementen ist Axiom I eine Folge des Axiomes II.

Ein zweites Beispiel erweise die Unabhängigkeit des Axiomes II von den Axiomen I und III.

Das System enthalte n Elemente $a_1, a_2, \ldots, a_n$, für die Verknüpfung gelte

$$a_i \,.\, a_k = a_k \,.$$

Hier sind Axiom I und III erfüllt, dagegen II nicht.

Jede assoziative Gruppe, die mehr als ein Element enthält, ist ein Beispiel für die Unabhängigkeit des Axioms III von den Axiomen I und II. Wir werden nämlich zeigen, daß eine solche assoziative Gruppe nicht distributiv sein kann.

Die Widerspruchslosigkeit der Axiome I, II und III beweist man durch Aufstellung distributiver Gruppen.

1. *Beispiel*: Das System der Elemente seien die komplexen Zahlen. Die Verknüpfung $a \,.\, b$ ordne den Zahlen a und b die Zahl

$$a \,.\, b = \alpha\, a + \beta\, b$$

zu, wobei α und β festgewählte Zahlen sind, deren Summe $\alpha + \beta = 1$ ist.

2. *Beispiel*: Das System der Elemente seien die reellen positiven Zahlen, die Null ausgeschlossen, die Verknüpfung $a \,.\, b$ ordne den Zahlen a und b die Zahl $a \,.\, b = \sqrt{ab}$ (das geometrische Mittel) zu, oder allgemeiner $a^\alpha b^\beta$ mit $\alpha + \beta = 1$, α und β von Null verschiedene reelle Zahlen. Dabei ist $a^\alpha = e^{\alpha \ln a}$.

3. *Beispiel*: Das System der Elemente seien die Punkte des n-dimensionalen affinen Raumes. Die Verknüpfung $a \,.\, b$ ordne den Punkten a und b einen Punkt der Strecke $\overline{ab}$ zu, der diese Strecke nach einem gegebenen Verhältnisse $\alpha : \beta$ teilt (z. B. den Mittelpunkt der Strecke $\overline{ab}$).

4. *Beispiel*: Das System der Elemente seien die Punkte des n-dimensionalen projektiven Raumes mit Ausnahme der Punkte einer $(n-1)$-dimensionalen Hyperebene E_{n-1} dieses Raumes [1]).

Der Punkt $a \,.\, b$ liege dann auf der Geraden ab so, daß das Doppelverhältnis $(a, b, a \,.\, b, c)$, wobei c der Schnittpunkt der Geraden ab mit der E_{n-1} ist, einen bestimmten festen Wert $\varkappa$ hat.

Führt man projektive Koordinaten ein, und seien $a_1, \ldots, a_{n+1}; b_1, \ldots, b_{n+1}$ die Koordinaten der Punkte a und b, $A_i x_i = 0$, $i = 1, \ldots, n+1$ die Gleichung der E_{n-1}, so hat der Punkt $a \,.\, b = d$ die projektiven Koordinaten

$$d_i = A_t\,(a_i b_t - \varkappa\, b_i a_t), \qquad i, t = 1, \ldots, n+1.$$

Aus dieser Formel ist der Gruppennachweis einfach zu erbringen, wir werden im § 2 eine sehr einfache Methode, diesen Nachweis zu führen, geben.

Bevor wir daran gehen, Beispiele endlicher distributiver Gruppen zu geben, das sind Gruppen, die nur endlich viele Elemente enthalten, sei eine charakteristische Eigenschaft distributiver Gruppen besprochen. In einer assoziativen Gruppe ist bekanntlich ein Element, das Einheitselement ausgezeichnet, für dieses — es sei mit e bezeichnet — gilt

$$a \,.\, e = e \,.\, a = a$$

für jedes Element a der assoziativen Gruppe. In einer distributiven Gruppe dagegen gibt es keine ausgezeichneten Elemente, in einer solchen herrscht vielmehr *eine Homogenität* der Art, daß eine gruppentheoretische Eigenschaft, die einem Elemente einer solchen Gruppe zukommt, jedem Elemente dieser Gruppe zukommen muß (§ 2).

Wir wollen zeigen, daß eine distributive Gruppe, die mehr als ein Element enthält, kein Einheitselement enthalten kann. Setzen wir in eine der beiden Relationen des Axioms III $b = c = a$, wobei a ein beliebiges Element der Gruppe sei, so folgt aus $(a \,.\, a) \,.\, a = (a \,.\, a) \,.\, (a \,.\, a)$ wegen des zweiten Axiomes die wichtige Relation

$$a \,.\, a = a,$$

die also für jedes Element einer distributiven Gruppe zu gelten hat. Wäre nun in der Gruppe ein Einheitselement e vorhanden, so hätte $a \,.\, e = a \,.\, a$, $e = a$ zur Folge, d. h. jedes Element dieser Gruppe wäre das Einheitselement, diese Gruppe könnte also nur dieses Element enthalten, q. e. d.

---

[1]) *Dual*: Das System der Elemente seien die E_{n-1} eines projektiven R_n mit Ausnahme der E_{n-1}, die durch einen bestimmten Punkt des R_n gehen.

Die Gruppe, die nur ein Element a enthält, für das nach Axiom I $a \,.\, a = a$ zu gelten hat, ist das einzige Beispiel einer Gruppe, die zugleich assoziativ und distributiv ist.

(Eine solche Gruppe kann nur ein Element enthalten, sonst könnte sie als distributive Gruppe das Einheitselement nicht enthalten, dagegen als assoziative müßte sie es enthalten.)

Eine distributive Gruppe, die nur zwei Elemente enthält, gibt es nicht. Seien a und b diese zwei Elemente, so folgt aus $a \,.\, a = a$, $b \,.\, b = b$, daß $a \,.\, b$ weder a noch b sein kann, daß also Axiom I nicht erfüllbar ist.

Dagegen gibt es eine distributive Gruppe von drei Elementen, — sie ist kommutativ.

Seien a, b, c die Elemente dieser Gruppe, so gilt $a \,.\, a = a$, $b \,.\, b = b$, $c \,.\, c = c$. $a \,.\, b$ kann weder a noch b, muß also gleich c sein. Ebenso ist $b \,.\, a = c$. Das *Cayley*schema der Gruppe ist:

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

Anschließend zeigen wir, daß jede endliche kommutative distributive Gruppe von ungerader Ordnung ist.

Sei $G\{a_1, a_2, \ldots, a_n\}$ eine kommutative distributive Gruppe der Ordnung n. Wir heben ein beliebiges Element, z. B. a_1, heraus und fassen das Restsystem $a_2, a_3, \ldots, a_n$ ins Auge.

Sei a_i ein Element dieses Restsystems, so gibt es in G ein „zugeordnetes" Element $a_{\sigma i}$ für das

$$a_i \,.\, a_{\sigma i} = a_1 \qquad \text{ist.}$$

Da $a_i \neq a_1$ ist, so ist $a_{\sigma i}$ von a_1 und a_i verschieden. Das a_i zugeordnete Element ist demnach ein von a_i verschiedenes Element des Restsystemes. Dem Element $a_{\sigma i}$ ist — wegen der Kommutativität der Gruppe — wieder das Element a_i zugeordnet. Die Elemente des Restsystemes $a_2, \ldots, a_n$ sind somit in zugeordnete Elemente gepaart, ihre Anzahl ist daher gerade. Die Ordnung der kommutativen Gruppe selbst ist ungerade, q. e. d.

Dagegen gibt es zu jeder ungeraden Zahl $N = 2n + 1$ eine kommutative Gruppe dieser Ordnung.

Mit $1, 2, 3, \ldots, 2n + 1$ bezeichnen wir die Elemente dieser Gruppe, die Verknüpfung $a \,.\, b$ ordne den Elementen a und b das Element zu, das der Gleichung

$$a \,.\, b \equiv (n + 1)(a + b) \qquad \mod (2n + 1)$$

genügt. Man überzeugt sich leicht, daß eine kommutative Gruppe vorliegt.

Man kann diese kommutative Gruppe $(2n + 1)$-ter Ordnung anschaulich deuten, sobald man sie isomorph auf die Endpunkte des regulären $(2n + 1)$-Ecks abbildet. Das Verknüpfungselement $c = a \,.\, b$ liegt dann stets auf der Streckensymmetralen der Eckpunkte a und b.

Beweis: Da $a(n + 1) \equiv \dfrac{a}{2} \mod (2n + 1)$ ist, können wir die Verknüpfungsvorschrift in der Form

$$a \,.\, b \equiv \frac{a + b}{2} \qquad \mod (2n + 1)$$

ansetzen. Sei nun $a < b$, so sei:

1. $\qquad b = a + 2d, \qquad c \equiv \dfrac{2a + 2d}{2} \equiv a + d \mod (2n + 1),$

also $c = a + d, \quad b = c + d.$

2. $\quad b = a + 2d + 1, \quad c \equiv \dfrac{a + b + 2n + 1}{2} \equiv a + d + n + 1 \equiv b + (n - d) \mod (2n + 1),$

also $c = b + (n - d), \quad c + (n - d) = b + 2(n - d) = a + 2n + 1 \equiv a,$ q. e. d.

Wenn es auch kommutative Gruppen gerader Ordnung nicht gibt, so gibt es doch nicht kommutative; die *Gruppe vierter Ordnung* sei ein Beispiel. Wenn wir mit a_1, a_2, a_3, a_4 die Elemente bezeichnen, so können wir stets $a_1 . a_2 = a_3$ ansetzen ($a_1 . a_2$ kann nur a_3 oder a_4 sein, wir können durch event. Umnumerierung stets $a_1 . a_2 = a_3$ erreichen).

Im *Cayley*schema sind somit folgende Verknüpfungen bekannt:

	a_1	a_2	a_3	a_4
a_1	a_1	a_3	.	.
a_2		a_2		
a_3			a_3	
a_4				a_4

In der ersten Zeile sind an die beiden freien Stellen a_2 und a_4 zu setzen, a_4 kann an letzter Stelle wegen $a_4 . a_4 = a_4$ nicht stehen, somit muß $a_1 . a_3 = a_4$ und $a_1 . a_4 = a_2$ sein. Mit Hilfe des Axiomes II ist man aber dann schon in der Lage die übrigen freien Stellen des Schemas auszufüllen und erhält:

	a_1	a_2	a_3	a_4
a_1	a_1	a_3	a_4	a_2
a_2	a_4	a_2	a_1	a_3
a_3	a_2	a_4	a_3	a_1
a_4	a_3	a_1	a_2	a_4

An der Hand des Schemas beweist man nun leicht die Gültigkeit des Axioms III. Es gibt also eine und nur eine distributive Gruppe der Ordnung vier.

Gruppen der Ordnung fünf gibt es, eine — die kommutative — haben wir eben aufgestellt, eine Gruppe der Ordnung sechs gibt es wieder nicht. Die Aufgabe alle Gruppen einer bestimmten Ordnung aufzustellen, scheint ebenso kompliziert zu sein wie die entsprechende bei den assoziativen Gruppen.

Im § 3 geben wir weitere Beispiele.

§ 2. Die Homogenität distributiver Gruppen.

Sei G eine distributive Gruppe und A

$$A\{a_1, a_2, \ldots\}$$

eine Untergruppe von G. (Sie muß nicht abzählbar sein, nur der einfacheren Schreibweise wegen haben wir die Elemente numeriert.)

Sei dann p irgendein Element von G, so ist

$$B = A . p, \quad \text{das ist der Inbegriff} \quad \{b_1 = a_1 . p, b_2 = a_2 . p, \ldots\},$$

eine zur Gruppe A isomorphe Untergruppe von G.

Dabei nennen wir — in der Bezeichnungsweise der klassischen Gruppentheorie — zwei Gruppen $\{a_1, a_2, \ldots\}$ und $\{b_1, b_2, \ldots\}$ einstufig isomorph, sobald eine ein-eindeutige Zuordnung ihrer Elemente $a_i \rightleftarrows b_i$ der Art hergestellt werden kann, daß dem Verknüpfungsresultat $a_i . a_k$ von a_i und a_k das Verknüpfungsresultat $b_i . b_k$ der a_i und a_k zugeordneten Elemente b_i und b_k zugeordnet ist.

Beweis: Ist A eine Gruppe endlicher Ordnung, so folgt aus $a_i . a_k = a_l$ durch rechts-

seitige Verknüpfung mit $p : b_i \,.\, b_k = b_l$. Das *Cayley*schema *des Systemes* $\{b_1, b_2, \ldots\}$ entspricht somit dem *Cayley*schema *der Gruppe* $\{a_1, a_2, \ldots\}$ und fällt mit diesem zusammen, sobald man den Buchstaben b durch den Buchstaben a ersetzt. Damit ist aber bewiesen, daß B eine zu A isomorphe Untergruppe von G ist.

Für nicht endliche Gruppen gilt der Beweis ebenfalls durch sinngemäße Übertragung des Begriffes des *Cayley*schemas auf solche Gruppen.

Für $A \equiv G$ lautet das Resultat: *Ist p irgend ein Element von G, so ist durch die Zuordnung $a_i \leftrightarrows a_i \,.\, p$ die Gruppe G auf sich selbst isomorph bezogen.*

Wir können p nach Axiom II stets so wählen, daß (a_i, a_k fest gewählte Elemente) $a_i \,.\, p = a_k$ ist, daraus folgt:

Eine distributive Gruppe läßt sich einstufig isomorph auf sich so beziehen, daß einem Elemente a_i das beliebige Element a_k zugeordnet ist.

Daraus folgt die „Homogenität" distributiver Gruppen.

Es gibt keine gruppentheoretische Eigenschaft, die einem Elemente einer distributiven Gruppe zukäme, ohne für alle Elemente dieser Gruppe zu gelten.

1. *Folgerung*: Kommt ein Element a_i in h verschiedenen (und in nicht mehr als h verschiedenen) v-gliedrigen Untergruppen (d. h. Untergruppen der Ordnung v) einer Gruppe G vor, so trifft dies für jedes Element der Gruppe zu.

Enthalte demnach G, eine endliche Gruppe der Ordnung N, n solche v-gliedrige Untergruppen

$$A_1, A_2, \ldots, A_n$$

so ist in dieser Gesamtheit jedes Element von G in derselben Anzahl h vorhanden. Somit gilt $Nh = nv$.

2. *Folgerung*: Sei wieder A_1 eine v-gliedrige Untergruppe von G (Gruppe N-ter Ordnung) und

$$A_2, A_3, \ldots, A_m$$

die Gesamtheit der zu A_1 isomorphen Untergruppen von G. Infolge der Definition isomorpher Gruppen sind damit je zwei Gruppen des Systems

$$(\alpha) \qquad A_1, A_2, \ldots, A_m$$

isomorph. *$A_i \,.\, p$ ist zu A_i also zu jeder der Gruppen dieses Systemes isomorph, also selbst eine Gruppe des Systemes.*

Kommt also ein Element a_i in q Gruppen (α) vor, so trifft dies für jedes Element von G zu.

Zählen wir somit alle Elemente von G, die in den Gruppen (α) enthalten sind ab, so erhalten wir

$$Nq = mv.$$

Wir diskutieren den interessanten Fall $q = 1$, für den die Gruppe G durch die Gruppen des Systemes (α) sich darstellen läßt

$$G = A_1 + A_2 + \cdots + A_m \,.$$

Bezeichnen wir mit A irgend eine der Untergruppen $A_1, \ldots, A_m$, so fällt die Gesamtheit der *verschiedenen* Untergruppen der Gesamtheit

$$A \,.\, a, A \,.\, b, \ldots \text{ usw., wo } G = \{a, b, \ldots\}$$

ist, mit den Gruppen (α) zusammen.

Unser Satz läßt sich dann folgendermaßen aussprechen:

Ist A eine Untergruppe von G der Eigenschaft, mit keiner von A verschiedenen und mit A isomorphen Untergruppe ein Element gemeinsam zu haben, so gilt die Zerlegung

$$G = A + A \,.\, \beta + A \,.\, \gamma + \cdots + A \,.\, \varepsilon.$$

Die Untergruppen A, $A \,.\, \beta, \ldots$ *usw., als Elemente betrachtet, bilden selbst eine distributive Gruppe* Γ, *und* G *ist* ν*-stufig isomorph zu* Γ.

Um diese Behauptung zu verstehen, müssen wir das Verknüpfungsresultat zweier Gruppen $C\{c_1, c_2, \ldots\}$ und $D\{d_1, d_2, \ldots\}$ erklären. *Unter* $C \,.\, D$ *verstehen wir den Inbegriff der Elemente* $c_i \,.\, d_k$, $i, k = 1, 2, \ldots$ *Wir haben* (*Axiom I*) *zu beweisen*, daß $A_i \,.\, A_k$ ein A_l, d. h. eine Gruppe des Systems (α) ist.

Wir bezeichnen mit $a_1^r, a_2^r, \ldots, a_\nu^r$ die Elemente der Gruppe A_r, $r = 1, \ldots, m$ und betrachten die beiden isomorphen Gruppen

$$a_1^i \,.\, A_k \quad \text{resp.} \quad A_i \,.\, a_l^k,$$

die im System (α) enthalten sind. Sie haben das Element $a_1^i a_l^k$ gemeinsam und müssen demnach zusammenfallen. Also gilt

$$A_l = a_1^i \,.\, A_k = A_i \,.\, a_1^k = A_i \,.\, a_2^k = \cdots = A_i \,.\, A_k,$$

und Axiom I ist nachgewiesen.

Um Axiom II zu beweisen, ist zu zeigen, daß die Gleichung

$$A_i \,.\, X = A_l$$

innerhalb des Systems (α) eine und nur eine Lösung zuläßt.

Nun gibt es in G ein Element $x = a_l^k$, das der Gleichung $a_1^i \,.\, a_1^k = a_1^l$ genügt. Daraus folgt aber $A_i \,.\, A_k = A_l$, also $X = A_k$. Gäbe es noch eine zweite Lösung A_j, gälte also $A_i \,.\, A_j = A_i \,.\, A_k$, so folgt daraus $a_1^i \,.\, A_j = a_1^i \,.\, A_k$ und somit $A_j = A_k$. Somit ist auch Axiom II bewiesen. Für $Y \,.\, A_l = A_k$ beweist man es in der gleichen Weise.

Der Nachweis des Axioms III ist ebenso einfach: $(A_i \,.\, A_k) \,.\, A_l$ ist eine Gruppe von (α), ebenfalls $(A_i \,.\, A_l) \,.\, (A_k \,.\, A_l)$. Beide Gruppen enthalten das Element

$$(a_1^i \,.\, a_1^k) \,.\, a_1^l = (a_1^i \,.\, a_1^l) \,.\, (a_1^k \,.\, a_1^l)$$

und fallen somit zusammen.

Wir bringen drei Beispiele von Systemen isomorpher Untergruppen, für die $q = 1$ *ist.*

1. *Beispiel*: A ist eine ν-gliedrige Untergruppe der Gruppe N-ter Ordnung G der Eigenschaft, mit keiner von A verschiedenen Untergruppe ν-ter Ordnung ein Element gemeinsam zu haben.

Dann kann auch A mit keiner von A verschiedenen und mit A isomorphen Untergruppe ein Element gemeinsam haben, und die Bedingungen des Satzes sind erfüllt.

2. *Beispiel*: Sei G eine Gruppe N-ter Ordnung und a_1 ein Element von G. Wir behaupten: Die Elemente x von G, die die Gleichung

$$a_1 \,.\, x = x \,.\, a_1$$

befriedigen, bilden eine Untergruppe A von G, die mit keiner isomorphen ein Element gemeinsam hat.

Da die Lösungselemente $x = a_1, a_2, \ldots$ in endlicher Zahl vorhanden sind, so ist des Gruppennachweises wegen nur die Gültigkeit des Axioms I zu überprüfen. Nun folgt aus $a_1 \,.\, x = x \,.\, a_1$ und $a_1 \,.\, y = y \,.\, a_1 : a_1 \,.\, (x \,.\, y) = (x \,.\, y) \,.\, a_1$; d. h. mit x und y ist $x \,.\, y$ auch eine Lösung. Bezeichnen wir die Untergruppe der Lösungen mit

$$A : \{a_1, a_2, \ldots, a_\nu\}$$

so muß, da a_1 mit jedem Element der Gruppe A vertauschbar ist, dies für jedes andere Element der Gruppe gelten. [Vertauschbar im Sinne: $a_1 \,.\, a_i = a_i \,.\, a_1$]. Heben wir aus A also irgend ein Element a_i heraus, so stellt A die Gesamtheit der mit a_i vertauschbaren Elemente von G dar, denn jedes Element, das mit a_i vertauschbar ist, ist mit a_1 vertauschbar.

Sei dann B eine zu A isomorphe Untergruppe. Sie ist ebenfalls ν-ter Ordnung und enthält wegen der Homogenität der Gruppe G die Gesamtheit aller Elemente, die mit einem

beliebigen Elemente von B kommutativ sind. Haben A und B ein Element gemeinsam, so müssen sie zusammenfallen, da durch dieses Element A und B eindeutig definiert ist. Unsere Behauptung ist erwiesen.

Ehe wir ein drittes Beispiel behandeln, führen wir eine neue Bezeichnung ein. Wir schreiben

$$a \,.\, (a \,.\, b) = \overset{2}{a} \,.\, b$$

$$a \,.\, [a \,.\, (a \,.\, b)] = \overset{3}{a} \,.\, b, \ldots \text{ usw.}$$

3. *Beispiel.* Sei G eine Gruppe N-ter Ordnung und a_1 ein Element von G. Wir behaupten: Die Elemente x von G, die der Gleichung

$$\overset{r}{a}_1 \,.\, x = x$$

genügen, bilden eine Untergruppe A von G, die mit keiner isomorphen ein Element gemeinsam hat. Der Gruppennachweis wird wie im Beispiele 2 erbracht. Bezeichnen wir die Gruppe der Lösungen mit

$$A\{a_1, a_2, \ldots, a_\nu\}\,^{1}),$$

so muß, da $\overset{r}{a}_1 \,.\, a_i = a_i$ $(i = 1, 2, \ldots, \nu)$ gilt, wegen der Homogenität von A $\overset{r}{a}_t \,.\, a_i = a_i$ $(i = 1, 2, \ldots, \nu)$ für $t = 1, 2, \ldots, \nu$ gelten, d. h. die Gruppe A ist durch irgend eines ihrer Elemente a_t infolge $\overset{r}{a}_t \,.\, x = x$ eindeutig fixiert. Sei dann $B = \{b_1, b_2, \ldots, b_\nu\}$ eine zu A isomorphe Untergruppe von G, so ist sie durch irgend ein Element b_t und die Gleichung $\overset{r}{b}_t \,.\, x = x$ eindeutig fixiert [2]). Haben somit A und B ein Element gemeinsam, so fallen sie zusammen.

Bemerkung: Wir hätten anstelle der Gleichung $\overset{r}{a}_1 \,.\, x = x$ eine Gleichung

$$a_1 \,.\, [(x \,.\, a_1) \,.\, a_1] = x \,.\, a_1$$

oder eine ähnliche (x darf rechts und links nur einmal auftreten) setzen können.

§ 3. Erzeugungsprinzipien distributiver Gruppen.

A. Erzeugung aus assoziativen kommutativen Gruppen.

Sei $G_a\{a_1, a_2, \ldots, a_{2n+1}\}$ eine assoziative kommutative Gruppe der Ordnung $2n + 1$, sei ferner α eine ganze Zahl und α und $\alpha - 1$ relativ prim zu $2n + 1$ (z. B. $\alpha = 2$, $\alpha = n + 1$). Das Verknüpfungsresultat der Elemente a_i und a_k der Gruppe G_a bezeichnen wir mit

$$a_i \circ a_k,$$

dann gilt nach Voraussetzung $a_i \circ a_k = a_k \circ a_i$, $(a_i \circ a_k) \circ a_l = a_i \circ (a_k \circ a_l)$. Mit a_i^α bezeichnen wir das Element $a_i \circ a_i \circ \ldots \ldots \circ a_i$, α-mal iteriert. *Durchläuft i die Reihe* $1, 2, \ldots, 2n + 1$, *so durchläuft a_i^α alle Elemente von G_a.* Im entgegengesetzten Falle würde für $a_i \neq a_k$, $a_i^\alpha = a_k^\alpha$ gelten. Bezeichnen wir mit a_k^{-1} wie üblich das inverse Element von a_k in G_a, so folgt

$$a_i^\alpha \circ (a_k^{-1})^\alpha = 1 = (a_i \circ a_k^{-1})^\alpha.$$

$a_i \circ a_k^{-1}$ kann nicht das Einheitselement sein, sonst gälte $a_k^{-1} = a_i^{-1}$, also $a_k = a_i$ gegen Voraussetzung. Bezeichnen wir $a_i \circ a_k^{-1} = a_l$, so erfüllt a_l die Gleichung $a_l^\alpha = 1$; daraus folgt, daß es in G_a eine Untergruppe der Ordnung ν geben müßte, wobei ν ein Teiler von α wäre. Da aber dann ν auch Teiler von $2n + 1$ sein müßte, so wären gegen die Voraussetzung α und $2n + 1$ nicht relativ prim. Somit ist die Gleichung $x^\alpha = a_i$, also $x = \overset{\frac{1}{\alpha}}{a_i}$ [3]) eindeutig in G_a lösbar. Dasselbe gilt natürlich für $\alpha - 1$ anstelle von α.

---

[1]) Wir wollen die Zahl r den Grad der Gruppe ν-ter Ordnung A nennen.

[2]) Infolge der Homogenität der Gesamtgruppe G.

[3]) Wir können in der Reihe $1, 2, \ldots, 2n+1$ immer eine Zahl β finden, daß $\overset{\frac{1}{\alpha}}{a} = a^\beta$ ist. In der Tat,

Wir zeigen nun, daß wir die Elemente von G_a als Elemente einer distributiven Gruppe G_a der Ordnung $2n+1$ auffassen können, wenn wir als neue Verknüpfungsoperation

$$a_i \,.\, a_k = a_i^{\alpha} \circ a_k^{1-\alpha}$$

ansetzen. Die Axiome I und II sind infolge unserer Voraussetzungen erfüllt, somit bleibt uns nur, den Nachweis für das Axiom III zu erbringen. Nun ist

$$(a_i \,.\, a_k) \,.\, a_l = (a_i^{\alpha} \circ a_k^{1-\alpha})^{\alpha} \circ a_l^{1-\alpha} = a_i^{\alpha^2} \circ a_k^{\alpha(1-\alpha)} \circ a_l^{1-\alpha},$$

ferner ist

$$(a_i \,.\, a_l) \,.\, (a_k \,.\, a_l) = (a_i^{\alpha} \circ a_l^{1-\alpha})^{\alpha} \circ (a_k^{\alpha} \circ a_l^{1-\alpha})^{1-\alpha} = a_i^{\alpha^2} \circ a_k^{\alpha(1-\alpha)} \circ a_l^{1-\alpha}.$$

Also gilt Axiom III, q. e. d.

Erste Bemerkung: Für die spezielle, kommutative Gruppe G_a $(2n+1)$-ter Ordnung, deren Elemente $1, 2, \ldots, 2n+1$ der Verknüpfung $a \circ b \equiv a + b \mod 2n+1$ unterliegen, ist $a^{\alpha} = \alpha a$, also

$$a \,.\, b \equiv \alpha a + (1-\alpha) b \mod 2n+1.$$

Beispiel 1, § 1.

Zweite Bemerkung: Betrachten wir die nichtendliche kommutative G_a, deren Elemente alle reellen Zahlen sind und deren Verknüpfungsgesetz $a \,.\, b = a + b$ ist, so ist ebenfalls $a \,.\, b = \alpha a + \beta b$ mit $\alpha + \beta = 1$ das Verknüpfungsgesetz der entsprechenden distributiven Gruppe.

Dritte Bemerkung: Sei A_a eine Untergruppe ν-ter Ordnung von G_a, dann ist ν als Teiler von $2n+1$ zu α und $\alpha - 1$ relativ prim. Sind $b_1, b_2, \ldots, b_\nu$ die Elemente von A_a, so bildet dieses System vermöge der Verknüpfung

$$b_i \,.\, b_k = b_i^{\alpha} \circ b_k^{1-\alpha}$$

eine distributive Gruppe, d. h. *die Elemente einer Untergruppe A_a der Gruppe G_a bilden eine Untergruppe A_d der Gruppe G_d.*

Die Elemente

$$A_d \,.\, p = \{b_1 \,.\, p, b_2 \,.\, p, \ldots, b_\nu \,.\, p\} = \{b_1^{\alpha} \circ p^{1-\alpha}, \ldots, b_\nu^{\alpha} \circ p^{1-\alpha}\} = \{b_1^{\alpha}, \ldots, b_\nu^{\alpha}\} \circ p^{1-\alpha} = A^{\alpha} \circ p^{1-\alpha}$$

der distributiven Untergruppe $A_d \,.\, p$ bilden eine „Nebengruppe“ $A_a \circ p^{1-\alpha}$ der Untergruppe A_a von G_a. Somit: Haben $A_d \,.\, p$ und $A_d \,.\, q$ ein Element gemeinsam, so fallen sie zusammen, und es gilt die Zerlegung:

$$G_d = A_d + A_d \,.\, p + \cdots + A_d \,.\, t.$$

Sei nun

$$b_i \,.\, p = b_i^{\alpha} \circ p^{1-\alpha} \text{ ein Element von } A_d \,.\, p$$
$$b_j \,.\, q = b_j^{\alpha} \circ q^{1-\alpha} \text{ ein Element von } A_d \,.\, q,$$

dann ist

$$(b_i \,.\, p) \,.\, (b_j \,.\, q) = (b_i^{\alpha} \circ p^{1-\alpha})^{\alpha} \circ (b_j^{\alpha} \circ q^{1-\alpha})^{1-\alpha} =$$
$$= (b_i^{\alpha} \circ b_j^{1-\alpha})^{\alpha} \circ (p^{\alpha} \circ q^{1-\alpha})^{1-\alpha} = (b_i \,.\, b_j) \,.\, (p \,.\, q).$$

Da aber dieses Element in der Gruppe $A_d \,.\, (p \,.\, q)$ liegt, so bilden die Untergruppen

$$A_d, A_d \,.\, p, \ldots, A_d \,.\, t,$$

als Elemente betrachtet, selbst eine distributive Gruppe. (Axiom II und III sind erfüllt, Beweis wie früher.)

Ferner gilt die Verknüpfungsgleichung:

---

aus $a = a^{\alpha\beta}$ folgt $a^{\alpha\beta-1} = 1$. Nun ist dies stets für $\alpha\beta - 1 = 2n+1$ der Fall, also für $\alpha\beta \equiv 1 \mod (2n+1)$, und da α relativ prim zu $2n+1$ ist, gibt es ein solches β.

$$(b_i \,.\, p) \,.\, (b_j \,.\, q) = (b_i \,.\, b_j) \,.\, (p \,.\, q).$$

Sind $B_d\colon \{b_1, \ldots, b_\mu\}$, $C_d\colon \{c_1, \ldots, c_\nu)$ zwei Untergruppen von G_d, so folgt aus

$$(b_i \,.\, c_k) \,.\, (b_j \,.\, c_l) = (b_i \,.\, b_j) \,.\, (c_k \,.\, c_l)$$

der Gruppencharakter des Elementsystemes

$$\{\ldots, (b_i \,.\, c_k), \ldots\}, \quad i = 1, \ldots, \mu, \; k = 1, \ldots, \nu.$$

B. Erzeugung distributiver Gruppen aus distributiven Gruppen.

(Gilt auch für assoziative Gruppen.)

Seien $A\,\{a_1, \ldots, a_\nu\}$ mit der Verknüpfung $a_i \,.\, a_k$ und
$B\,\{b_1, \ldots, b_\mu\}$ mit der Verknüpfung $b_i \bigcirc b_k$
zwei distributive Gruppen der Ordnung ν resp. μ, so bildet das Elementsystem $\{\ldots, (a_i, b_k), \ldots\}$ mit der Verknüpfung $(a_i, b_k) \times (a_j, b_l) = (a_i \,.\, a_j, b_k \bigcirc b_l)$ eine distributive Gruppe der Ordnung $\mu\nu$. Man überzeugt sich sofort, daß die Axiome I bis III erfüllt sind.

Eine so konstruierte Gruppe, deren Elemente (a_i, b_k) durch zwei Indizes numeriert sind, wollen wir eine *Zweiindizesgruppe* nennen.

Analog kann man *Dreiindizesgruppen* usw. bilden.

Bemerkung: Setzen wir statt der Verknüpfung $a \,.\, b = a^\alpha \circ b^{1-\alpha}$ die Verknüpfung $a \,.\, b = a^\alpha \circ b^\beta$, wobei α, β relativ prim zu $2n + 1$ sind, so sind im entsprechenden *Cayley*schema Axiom I und II erfüllt, an Stelle von III tritt

$$(a \,.\, d) \,.\, (b \,.\, d) = (a \,.\, b) \,.\, (d \,.\, d), \text{ resp. } (d \,.\, a) \,.\, (d \,.\, b) = (d \,.\, d) \,.\, (a \,.\, b),$$

resp. die allgemeinere

$$(a \,.\, b) \,.\, (c \,.\, d) = (a \,.\, c) \,.\, (b \,.\, d).$$

Es gelten für solche Gruppen die in diesem Paragraphen aufgestellten Beziehungen zu den *Abel*schen Gruppen ungerader Ordnung.

Ist A eine Untergruppe, so stellt $A \,.\, p$ eine „Nebengruppe“ dar, wie bei den assoziativen Gruppen.

§ 4. Untergruppen, Indexsatz.

Definition der einfachen Gruppe: *Wir nennen eine Gruppe einfach, wenn sie keine echte Untergruppe der Ordnung größer als eins enthält.* Daraus folgt, daß eine einfache Gruppe durch irgend zwei ihrer Elemente vollständig bestimmt ist.

Sei $A\{a_1, \ldots, a_\nu\}$ eine einfache Untergruppe der Gruppe G und p ein beliebiges Element von G, so beweisen wir, daß $A \,.\, (A \,.\, p)$ eine ν-gliedrige Gruppe $A \,.\, t$ ist. Wir bezeichnen die Gruppe $A \,.\, p$ mit B $(a_i \,.\, p = b_i, \; i = 1, \ldots, \nu)$, dann gilt

$$a_i \,.\, b_1 = a_i \,.\, (a_1 \,.\, p) = (a_i \,.\, a_1) \,.\, b_i = a_j \,.\, b_i,$$

wenn $a_i \,.\, a_1 = a_j$ ist.

Sei nun $a_i \neq a_1$, dann ist auch $a_i \neq a_j$ und also $b_i \neq b_j$. Die Gruppen $a_j \,.\, B$ und $A \,.\, b_1$ sind mit A einstufig isomorph, also einfache Gruppen, sie haben die Elemente $a_j \,.\, b_1$ und $a_i \,.\, b_1 = a_j \,.\, b_i$ gemeinsam, fallen demnach als einfache Gruppen zusammen, d. h. es gilt

$$A \,.\, b_1 = a_j \,.\, B, \quad j = 2, 3, \ldots, \nu.$$

Genau so hätte man

$$A \,.\, b_2 = a_h \,.\, B, \quad h = 1, 3, 4, \ldots, \nu$$

abgeleitet, woraus

$$a_1 \,.\, B = a_2 \,.\, B = \cdots = a_\nu \,.\, B = A \,.\, B = A \,.\, (A \,.\, p)$$

folgt, q. e. d.

Wir wollen den Satz auf Untergruppen ausdehnen, die durch zwei (aber nicht beliebige zwei) ihrer Elemente gegeben sind.

Wir beweisen vorerst den Hilfssatz: Sei eine solche Untergruppe A gegeben, und a_l und a_k zwei sie bestimmende Elemente, so bestimmen sowohl a_l und a_j als auch a_k und a_j die Untergruppe, wobei $a_l \,.\, a_j = a_k$ ist.

Beweis: Durch a_l und a_j ist eine kleinste Gruppe $\bar{A}$ bestimmt, für die $\bar{A} \leqq A$ gilt; $\bar{A}$ enthält aber a_k, demnach A, somit gilt $\bar{A} \geqq A$, demnach $\bar{A} = A$, q. e. d.

Ebenso beweist man, daß a_k und a_j A bestimmen.

Wir gehen nun an den Beweis des Satzes. Die Gruppe A sei durch ihre Elemente a_l und a_k bestimmt, ferner sei wie oben

(1) $a_l \,.\, a_j = a_k$ gesetzt, dann gilt

(2) $a_k \,.\, b_j = (a_k \,.\, a_j) \,.\, b_k$ und

(3) $a_l \,.\, b_j = (a_l \,.\, a_j) \,.\, b_l = a_k \,.\, b_l = (a_k \,.\, a_l) \,.\, b_k$.

Die einstufig isomorphen Gruppen $A \,.\, b_j$ und $A \,.\, b_k$ enthalten die zwei Elemente $a_k \,.\, b_j = (a_k \,.\, a_j) \,.\, b_k$ sowie $a_l \,.\, b_j = (a_k \,.\, a_l) \,.\, b_k$.

Nun wird durch die Elemente $a_k \,.\, b_j$ und $a_l \,.\, b_j$ die Gruppe $A \,.\, b_j$ völlig bestimmt, ebenso bestimmen $(a_k \,.\, a_j) \,.\, b_k$ und $(a_k \,.\, a_l) \,.\, b_k$ völlig die Gruppe $A \,.\, b_k$, somit gilt $A \,.\, b_j = A \,.\, b_k$.

Seien nun $x_1, x_2, \ldots$ alle jene Elemente in G, für die $A \,.\, x_1 = A \,.\, x_2 = \cdots = A \,.\, b_j$ gilt, so bilden diese Elemente eine Untergruppe von G. Da ihre Anzahl endlich ist, so ist nur Axiom I nachzuweisen. Aus

$$A \,.\, (x_p \,.\, x_q) \leqq (A \,.\, x_p) \,.\, (A \,.\, x_q) = (A \,.\, x_p) \,.\, (A \,.\, x_p) = A \,.\, x_p = A \,.\, b_j$$

folgt die Gruppeneigenschaft. Diese Gruppe enthält aber b_j und b_k somit die Untergruppe B, also gilt

$$A \,.\, b_1 = A \,.\, b_2 = \cdots = A \,.\, b_\nu = A \,.\, B, \qquad \text{q. e. d.}$$

Sei nun $A\{a_1, a_2, \ldots, a_\nu\}$ eine Untergruppe der Eigenschaft, daß für irgendwelche zwei Elemente a_i und a_k von A eine Gleichung

$$a_i = \overset{2}{a}_k \cdot a_i$$

nicht bestehe, so ist $A \,.\, (A \,.\, p) = A \,.\, t$. Wir knüpfen an Formel 1, 2 und 3 an.

In $A \,.\, b_j$ sind die beiden Elemente $a_k \,.\, b_j = (a_k \,.\, a_j) \,.\, b_k$ und $a_l \,.\, b_j = (a_k \,.\, a_l) \,.\, b_k$ enthalten, dabei ist k ein beliebiger Index der Reihe $1, 2, \ldots, \nu$. Ihr Produkt $(a_l \,.\, a_k) \,.\, b_j = [a_k \,.\, (a_l \,.\, a_j)] \,.\, b_k = (a_k \,.\, a_k) \,.\, b_k = a_k \,.\, b_k$ ist somit in $A \,.\, b_j$ enthalten.

Jede der Gruppen $A \,.\, b_j$ enthält somit die folgenden Elemente

(4) $$a_1 \,.\, b_1, \quad a_2 \,.\, b_2 \quad , \ldots, a_\nu \,.\, b_\nu.$$

Sind diese Elemente alle verschieden, dann bestimmen sie genau die Gruppe $A \,.\, b_j$, und es gilt $A \,.\, b_1 = A \,.\, b_2 = \cdots = A \,.\, b_\nu = A \,.\, B$.

Wir wollen nun sehen, was aus

(4′) $$a_r \,.\, b_r = a_l \,.\, b_l$$

folgt. In A gibt es ein Element a_k für das

(4″) $$a_r \,.\, a_k = a_l$$

gilt. Nun ist

$$\begin{aligned} a_r \,.\, b_k &= (a_r \,.\, a_k) \,.\, b_r = a_l \,.\, b_r = (a_l \,.\, a_r) \,.\, b_l \\ &= (a_l \,.\, b_l) \,.\, (a_r \,.\, b_l) = (a_r \,.\, b_r) \,.\, (a_r \,.\, b_l) = a_r \,.\, (b_r \,.\, b_l), \end{aligned}$$

daraus folgt $b_k = b_r \,.\, b_l$, somit

(4‴) $$a_k = a_r \,.\, a_l.$$

Aus (4″) und (4‴) schließen wir $a_l = a_r \,.\, (a_r \,.\, a_l) = \overset{2}{a}_r \,.\, a_l$. Ebenso gilt natürlich $a_r = \overset{2}{a}_l \,.\, a_r$.

Nach Voraussetzung besteht zwischen den Elementen von A keine derartige Relation, somit folgt $A \,.\, (A \,.\, p) = A \,.\, t$, q. e. d.

Bemerkung: Wir zeigen, daß aus $a_l = \overset{2}{a}_r \,.\, a_l$ die Beziehung (4′) folgt. Wir setzen wieder $a_r \,.\, a_l = a_k$ und erhalten $a_l = a_r \,.\, a_k$. Nun ist

$$a_r \,.\, b_k = a_r \,.\, (b_r \,.\, b_l) = (a_r \,.\, b_r) \,.\, (a_r \,.\, b_l)\,,$$

ferner gilt auch

$$a_r \,.\, b_k = (a_r \,.\, a_k) \,.\, b_r = a_l \,.\, b_r = (a_l \,.\, a_r) \,.\, b_l = (a_l \,.\, b_l) \,.\, (a_r \,.\, b_l).$$

Der Vergleich ergibt $a_r \,.\, b_r = a_l \,.\, b_l$, q. e. d.

Ist $A\{a_1, \ldots, a_\nu\}$ eine kommutative Gruppe, die keine Untergruppe der Ordnung drei enthält, so gilt $A \,.\, (A \,.\, p) = A \,.\, t$.

Dies ist eine direkte Folge der vorhergehenden Betrachtung.

Bestünde eine Relation $a_j = a_i \,.\, (a_i \,.\, a_j)$, so folgt aus $a_i \,.\, a_j = a_k$, $a_j = a_i \,.\, a_k$. Ferner ist dann $a_j \,.\, a_k = (\ _i \,.\, a_k) \,.\, (a_i \,.\, a_j) = a_i \,.\, (a_k \,.\, a_j)$, woraus $a_j \,.\, a_k = a_i$ folgt, d. h. die Elemente a_i, a_j und a_k bilden eine Untergruppe der Ordnung 3, im Widerspruch zu unserer Voraussetzung.

1. *Satz*: *Für Untergruppen A, für die $A \,.\, (A \,.\, p) = A \,.\, t$ ist, gilt die Zerlegung*

$$G = A + A \,.\, p + A \,.\, q + \cdots + A \,.\, w.$$

Wir beweisen dies, indem wir zeigen, daß zwei Untergruppen $A \,.\, p$ und $A \,.\, q$ identisch oder elementfremd sind.

Beweis: Die beiden Untergruppen mögen ein Element c gemeinsam enthalten. Nun gilt

(5′) $A \,.\, (A \,.\, p) = A \,.\, c$ resp. (5″) $A \,.\, (A \,.\, q) = A \,.\, c$, somit $A \,.\, (A \,.\, p) = A \,.\, (A \,.\, q)$, also (5‴) $a_1 \,.\, (A \,.\, p) = a_1 \,.\, (A \,.\, q)$, also (5⁗) $A \,.\, p = A \,.\, q$, q. e. d.

Wir zeigen nun für spätere Zwecke, daß für eine einfache Untergruppe der Ordnung ν, $A\{a_1, a_2, \ldots, a_\nu\}$, auch $(A \,.\, p) \,.\, A$ eine ν-gliedrige Gruppe $t \,.\, A$ ist.

Es gilt

(6) $(a_i \,.\, p) \,.\, a_k = (a_i \,.\, a_k) \,.\, (p \,.\, a_k) = a_l \,.\, (p \,.\, a_k) = (a_l \,.\, p) \,.\, (a_l \,.\, a_k) = (a_l \,.\, p) \,.\, a_h$,

wobei

(6′) $a_i \,.\, a_k = a_l$ und (6″) $a_l \,.\, a_k = a_h$

ist. Ferner gilt

(7) $(a_l \,.\, p) \,.\, a_h = (a_l \,.\, a_h) \,.\, (p \,.\, a_h) = a_s \,.\, (p \,.\, a_h) = (a_s \,.\, p) \,.\, (a_s \,.\, a_h) = (a_s \,.\, p) \,.\, a_t$,

wobei

(7′) $a_l \,.\, a_h = a_s$ und (7″) $a_s \,.\, a_h = a_t$ ist. Für a_s und a_t berechnen wir

(8)
$$\begin{cases} a_s = a_l \,.\, a_h = (a_i \,.\, a_k) \,.\, (a_l \,.\, a_k) = (a_i \,.\, a_l) \,.\, a_k \\ a_t = a_s \,.\, a_r = [(a_i \,.\, a_l) \,.\, a_k] \,.\, (a_l \,.\, a_k) = [(a_i \,.\, a_l) \,.\, a_l] \,.\, a_k\,. \end{cases}$$

Die beiden einfachen Gruppen $(a_i \,.\, p) \,.\, A$ und $(A \,.\, p) \,.\, a_h$ haben die Elemente

(8′) $(a_i \,.\, p) \,.\, a_h$ und $(a_i \,.\, p) \,.\, a_k = (a_l \,.\, p) \,.\, a_h$ gemeinsam. Sei $a_i \neq a_k$, so ist nach (6′) $a_k \neq a_l$. Also ist nach (6″) $a_h \neq a_k$, d. h. die beiden Elemente (8′) sind verschieden.

$$(a_i \,.\, p) \,.\, A = (A \,.\, p) \,.\, a_h,$$

wobei $a_i \,.\, a_k = a_l$, $a_l \,.\, a_k = a_h$, also $(a_i \,.\, a_k) \,.\, a_k = a_h$ ist.

Nun sind zwei Fälle zu unterscheiden:

1. *Fall*: Für zwei Werte a_k (a_k und $a_{\bar{k}}$) seien a_h und $a_{\bar{h}}$ verschieden. Dann folgt

$$(A \,.\, p) \,.\, a_h = (A \,.\, p) \,.\, a_{\bar{h}} = (A \cdot p) \cdot A.$$

2. *Fall*: Wie man auch $k \neq i$ wähle, stets sei in $a_h = (a_i \,.\, a_k) \,.\, a_k$: a_h von a_k unabhängig. Dann muß $a_h = a_i$ sein, denn wäre $a_h = a_t$, $t \neq i$, so gälte $a_t = (a_i \,.\, a_t) \,.\, a_t$, d. h. $a_i \,.\, a_t = a_t$, d. h. $t = i$, was ein Widerspruch ist. Also muß

(9) $$a_i = (a_i \,.\, a_k) \,.\, a_k$$

gelten.

Nun war auch a_i völlig willkürlich, somit muß (9) für irgend zwei Elemente von A gelten (oder wir hätten den Fall 1). Dann aber folgt aus (8) $a_t = a_i \,.\, a_k$, und die einfachen Gruppen $(a_i \,.\, p) \,.\, A$ und $(A \,.\, p) \,.\, a_t$ enthalten die zwei verschiedenen Elemente $(a_i \,.\, p) \,.\, a_t$ und $(a_i \,.\, p) \,.\, a_k = (a_s \,.\, p) \,.\, a_t$. (Da $a_t \neq a_k$, wenn $a_i \neq a_k$ ist.) Es gilt also

(10) $$(a_i \,.\, p) \,.\, A = (A \,.\, p) \,.\, a_t.$$

Durchläuft k die Zahlen $1, 2, \ldots, i-1, i+1, \ldots, \nu$, so durchläuft t diese Zahlen in geänderter Folge, d. h. es gilt

$(a_i \,.\, p) \,.\, A = (A \,.\, p) \,.\, a_1 = (A \,.\, p) \,.\, a_2 = \cdots = (A \,.\, p) \,.\, a_x$, da ja a_i willkürlich gewählt war, q. e. d.

Sei $A\{a_1, \ldots, a_\nu\}$ eine Untergruppe und bestehen für keine zwei Elemente die Gleichungen $(a_i \,.\, a_p) \,.\, a_p = a_i$ oder $(a_p \,.\, a_i) \,.\, a_p = a_i$, so ist $(A \,.\, p) \,.\, A = t \,.\, A$. Wir beziehen uns auf die Formeln (6) bis (8). Die Gruppe $(a_i \,.\, p) \,.\, A$ enthält die Elemente $(a_i \,.\, p) \,.\, a_h$ und $(a_i \,.\, p) \,.\, a_k = (a_l \,.\, p) \,.\, a_h$, somit die Gesamtheit der Elemente $(x_r \,.\, p) \,.\, a_h$, wo x_r irgendein Element der die Elemente a_i und a_l umfassenden kleinsten Gruppe $\{a_i, a_l\}$ ist.

Dieser Gruppe gehören die Elemente a_k, a_h, a_s, a_t an, somit enthält $(a_i \,.\, p) \,.\, A$ die Elemente $(a_h \,.\, p) \,.\, a_h$, wobei $a_h = (a_i \,.\, a_k) \,.\, a_k$ ist.

Wir behaupten, daß mit a_k auch a_h alle Elemente von A durchläuft. Aus $(a_i \,.\, a_k) \,.\, a_k = (a_i \,.\, a_p) \,.\, a_p = a_r$ schließen wir wie folgt:

Setzen wir $a_i \,.\, a_k = a_l$, $a_i \,.\, a_p = a_q$, so gilt $a_l \,.\, a_k = a_q \,.\, a_p$, weiter ist $a_l \,.\, (a_p \,.\, a_k) = (a_i \,.\, a_k) \,.\, (a_p \,.\, a_k) = a_q \,.\, a_k$, ebenfalls gilt

$$a_l \,.\, (a_p \,.\, a_k) = (a_l \,.\, a_p) \,.\, (a_l \,.\, a_k) = (a_l \,.\, a_p)\,(a_q \,.\, a_p) = (a_l \,.\, a_q) \,.\, a_p = [a_i \,.\, (a_k \,.\, a_p)]a_p = \\ = a_q \,.\, [(a_k \,.\, a_p) \,.\, a_p],$$

der Vergleich ergibt somit $a_k = (a_k \,.\, a_p) \,.\, a_p$, was gegen die Voraussetzung ist. Also sind in $(a_i \,.\, p) \,.\, A$ alle Elemente

(γ) $$(a_1 \,.\, p) \,.\, a_1, \quad (a_2 \,.\, p) \,.\, a_2, \ldots, \quad (a_\nu \,.\, p) \,.\, a_\nu$$

enthalten.

Es sei nun, $b_t = a_t \,.\, p$ gesetzt, $b_l \,.\, a_l = b_k \,.\, a_k$.

Ist $a_r \,.\, a_k = a_l$, so bilden wir

$$b_r \,.\, a_k = (a_r \,.\, p) \,.\, a_k = a_l \,.\, (p \,.\, a_k) = b_l \,.\, (a_l \,.\, a_k) = (b_l \,.\, a_l) \,.\, (b_l \,.\, a_k) = \\ = (b_k \,.\, a_k) \,.\, (b_l \,.\, a_k) = (b_k \,.\, b_l) \,.\, a_k.$$

Das hätte nun $b_r = b_k \,.\, b_l$, also $a_r = a_k \,.\, a_l$ zur Folge, oder $(a_k \,.\, a_l) \,.\, a_k = a_l$, gegen die Voraussetzung. Somit enthalten alle Gruppen $(a_i \,.\, p) \,.\, A$ die *ν verschiedenen* Elemente (γ), und es gilt

$$(a_1 \,.\, p) \,.\, A = (a_2 \,.\, p) \,.\, A = \cdots = (a_\nu \,.\, p) \,.\, A = (A \,.\, p) \,.\, A, \quad \text{q. e. d.}$$

Folgerungen aus Satz 1.

1. Eine Gruppe der Ordnung einer Primzahl ist einfach.

2. Die Ordnung einer einfachen Untergruppe, einer Untergruppe, die durch zwei Elemente bestimmt ist, endlich einer Untergruppe, deren Elemente keiner Gleichung $a_i^2 \cdot a_k = a_k$ genügen, ist ein Teiler der Ordnung der Gruppe.

3. Für Untergruppen einer kommutativen Gruppe, deren Ordnung nicht durch drei teilbar ist, gilt der Indexsatz (die Ordnung der Untergruppe ist Teiler der Ordnung der Gruppe).

Zum Schlusse dieses Paragraphen notieren wir den

Satz: Ist $(A \,.\, p) \,.\, A = t \,.\, A$, so ist auch $A \,.\, (p \,.\, A) = A \,.\, \tau$, denn es gilt stets $(A \,.\, p) \,.\, A = A \,.\, (p \,.\, A)$.

Sei $(a_i \,.\, p) \,.\, a_k$ ein Element von $(A \,.\, p) \,.\, A$, so liegt es wegen

$$(a_i \,.\, p) \,.\, a_k = (a_i \,.\, a_k) \,.\, (p \,.\, a_k)$$

in $A \,.\, (p \,.\, A)$, somit ist

$$(A \,.\, p) \,.\, A \leqq A \,.\, (p \,.\, A).$$

Sei $a_i \,.\, (p \,.\, a_k) = (a_i \,.\, p) \,.\, (a_i \,.\, a_k)$ ein Element von $A \,.\, (p \,.\, A)$, so liegt es auch in $(A \,.\, p) \,.\, A$, somit gilt

$$(A \,.\, p) \,.\, A \geqq A \,.\, (p \,.\, A),$$

also ist $(A \,.\, p) \,.\, A = A \,.\, (p \,.\, A)$, q. e. d.

Bemerkung: Sei $G\{a_1, a_2, \ldots, a_\nu\}$ eine distributive Gruppe und die Gleichung $(a_i \,.\, a_k) \,.\, a_k = a_i$ innerhalb der Gruppe nicht erfüllbar. Wir definieren dann durch

$$a_i \circ a_k = (a_i \,.\, a_k) \,.\, a_k$$

eine neue Verknüpfung. Das System $\{a_1, \ldots, a_\nu\}$ erfüllt dann Axiom I und II und

$$(a_i \circ a_k) \circ (a_j \circ a_k) = [(a_i \,.\, a_k) \,.\, a_k] \circ [(a_j \,.\, a_k) \,.\, a_k]$$
$$= \{[(a_i \,.\, a_k) \,.\, a_k] \,.\, [(a_j \,.\, a_k) \,.\, a_k]\} \,.\, [(a_j \,.\, a_k) \,.\, a_k] = \{[(a_i \,.\, a_j) \,.\, a_k] \,.\, a_k\} \,.\, [(a_j \,.\, a_k) \,.\, a_k]$$
$$= \{[(a_i \,.\, a_j) \,.\, a_j] \,.\, a_k\} \,.\, a_k = (a_i \circ a_j) \circ a_k,$$

dagegen wird die linksseitige Distributivität im allgemeinen nicht erfüllt sein.

§ 5. Struktur der distributiven Gruppen.

Wir setzen in diesem Paragraphen voraus, daß für jede Untergruppe A von G $A \,.\, (A \,.\, p)$ und $(A \,.\, p) \,.\, A$ Untergruppen der Ordnung von A sind.

In Formeln: $\begin{cases} A \,.\, (A \,.\, p) = A \,.\, t \\ (A \,.\, p) \,.\, A = A \,.\, (p \,.\, A) = A \,.\, \tau. \end{cases}$

Diese Voraussetzung ist nach den Ergebnissen des § 4 jedenfalls für Gruppen G erfüllt, für die keine der Gleichungen

$$(x \,.\, y) \,.\, y = x, \quad (y \,.\, x) \,.\, y = x, \quad y \,.\, (y \,.\, x) = x$$

für zwei verschiedene Elemente x, y von G erfüllbar ist. Gruppen G dieser Eigenschaft wollen wir ausgezeichnete Gruppen nennen.

Bezeichnung: *Eine Untergruppe $A \,.\, p$ bezeichnen wir kurz $[A]$.*

Hilfssatz I: *Sind A, B und C Untergruppen der gleichen Ordnung ν, so folgt aus $A \cdot B = C$:*

$$B = [A],\ C = [A],\ A = [B],\ C = [B],\ A = [C],\ B = [C].$$

Beweis: Aus $A \,.\, B = C$ folgt $C = [A]$. Die Elemente von A seien mit a_t, von B mit b_t und von C mit c_t, $t = 1, 2, \ldots, \nu$ bezeichnet.

In G gibt es ein Element r für das $a_1 \,.\, r = b_1$ ist. Dann gilt

$$A \,.\, B = A \,.\, b_1 = A \,.\, (a_1 \,.\, r) = A \,.\, (A \,.\, r),$$

also $B = [A]$. Ferner sei $a_1 = b_1 \,.\, q$, dann gilt

$$C = A \,.\, B = a_1 \,.\, B = (b_1 \,.\, q) \,.\, B = (B \,.\, q) \,.\, B = B \,.\, (q \,.\, B),$$

somit $C = [B]$ und $A = [B]$.

Endlich ist $A \,.\, C = A \,.\, [A] = A \,.\, \sigma$, somit nach dem Vorhergehenden $A = [C]$, und ebenso folgt aus $B \,.\, C = B \,.\, [B] = B \,.\, \tau$, daß $B = [C]$ ist.

Hilfssatz II: *Sind A, B und C ν-gliedrige Untergruppen, so folgt aus $A \,.\, B =$ ν-gliedrige Untergruppe und $A = [C]$, $B = [C]$, daß $A \,.\, B = [C]$ ist.*

In der Tat ist $A = C \,.\, \varrho$, $B = C \,.\, \tau$, somit

$$A \,.\, B = (C \,.\, \varrho) \,.\, (C \,.\, \tau) \geqq C \,.\, (\varrho \,.\, \tau).$$

Da aber $A \,.\, B$ ν-gliedrig ist, so folgt $A \,.\, B = C \,.\, (\varrho \,.\, \tau) = [C]$.

Hilfssatz III: *Seien $A_1, A_2, \ldots, A_\sigma$ ν-gliedrige Untergruppen der Eigenschaft,*

daß die Produkte $A_i . A_k$, $(i, k = 1, \ldots, \sigma)$ *v-gliedrige Gruppen sind, und ergänzt man dieses System von v-gliedrigen Untergruppen durch Adjunktion jener Produkte* $A_i . A_k$, *die im System noch nicht vorhanden sind, so erhält man ein neues System* $A_1, A_2, \ldots, A_{\sigma+\tau}$ *der Eigenschaft, daß die Produkte* $A_i . A_k$, $i, k = 1, 2, \ldots, \sigma + \tau$ *ebenfalls v-gliedrige Gruppen sind.*

Wir haben nur zu beweisen, daß $A_i . A_{\sigma+k}$, $A_{\sigma+k} . A_i$ und $A_{\sigma+h} . A_{\sigma+k}$, $(i = 1, 2, \ldots, \sigma;\ h, k = 1, 2, \ldots, \tau)$ v-gliedrige Gruppen sind.

Aus $A_i . A_p =$ v-gliedriger Gruppe, folgt $A_i = [A_p]$, $i, p = 1, \ldots, \sigma$ (Hilfssatz I), und da $A_i . A_k$ eine v-gliedrige Gruppe ist, folgt nach Hilfssatz II:

$$A_i . A_k = [A_p],\ p, i, k = 1, 2, \ldots, \sigma.$$

Somit ist $A_{\sigma+k} = [A_i]$, denn es ist $A_{\sigma+k} = A_r . A_s$ nach Voraussetzung, also ist in der Tat $A_i . A_{\sigma+k}$ (ebenfalls dann $A_{\sigma+k} . A_i$) eine v-gliedrige Gruppe.

Daraus wieder schließen wir $A_i = [A_{\sigma+k}]$, $i = 1, \ldots, \sigma$, $k = 1, \ldots, \tau$. Sei nun $A_{\sigma+h} = A_p . A_q$, so ist $A_p = [A_{\sigma+k}]$ und $A_q = [A_{\sigma+k}]$, und da $A_p . A_q$ v-gliedrig ist, so ist (Hilfssatz II) $A_p . A_q = A_{\sigma+h} = [A_{\sigma+k}]$, somit sind $A_{\sigma+h} . A_{\sigma+k}$ $(h, k = 1, 2, \ldots, \tau)$ v-gliedrige Gruppen, q. e. d. Nun sind wir in der Lage den Satz zu beweisen:

Satz I: Seien $A_1, A_2, \ldots, A_\sigma$ *v-gliedrige Untergruppen der Eigenschaft, daß die Produkte* $A_i . A_k$ $(i = 1, 2, \ldots, \sigma)$ *v-gliedrig sind, so können wir eine distributive Gruppe, deren Elemente v-gliedrige Untergruppen sind, bilden, die* $A_1, \ldots, A_\sigma$ *als Elemente enthält.*

Beweis: Wir vervollständigen das System $A_1, A_2, \ldots, A_\sigma$ durch ihre Produkte $A_i . A_k$, sofern sie im System noch nicht enthalten sind, und erhalten ein neues System $A_1, \ldots, A_{\sigma+\tau}$, das wir in der gleichen Art vervollständigen und so weiter, bis wir zu einem System

$$(\alpha) \qquad A_1, A_2, \ldots, A_\varepsilon$$

gelangen der Eigenschaft, alle Produkte $A_i . A_k$ schon zu enthalten. Zu einem solchen System müssen wir der Endlichkeit der Grundgruppe G wegen gelangen, da alle Gruppen A_k, $k = 1, 2, \ldots, \varepsilon$ wegen $A_i . A_k$ v-gliedrig die Form $A_k = [A_1]$ haben und somit elementfremd sind [1]). Das System (α) genügt somit dem Axiom I. Sei A_i eine Untergruppe von (α), so durchläuft

$$A_i . A_k \text{ resp. } A_k . A_i \text{ mit } k = 1, 2, \ldots, \varepsilon$$

alle Elemente des Systems (α), denn aus

$$A_i . A_k = A_i . A_j \text{ folgt } a_1^i . A_k = a_1^i . A_j, \text{ also } A_k = A_j.$$

Somit ist Axiom II erfüllt.

Wir beweisen noch eine der beiden Relationen des Axioms III, z. B.

$$(A_i . A_k) . A_j = (A_i . A_j) . (A_k . A_j).$$

Die Gruppen $(A_i . A_k) . A_j$ und $(A_i . A_j) . (A_k . A_j)$ sind nach Axiom I in (α) enthalten und sind, da sie das Element $(a_1^i . a_1^k) . a_1^j = (a_1^i . a_1^j) . (a_1^k . a_1^j)$ gemeinsam haben, identisch.

Der Satz ist somit bewiesen.

Als Anwendung bringen wir den

Zusatz: Aus A und $A . p$ läßt sich stets eine distributive Gruppe bilden, deren Elemente Untergruppen der Form $A . h$ sind, und die als Elemente A und $A . p$ enthält.

$A_1 = A$ und $A_2 = A . p$ erfüllen in der Tat die Voraussetzungen des eben bewiesenen Satzes.

Bezeichnung: Sei G eine Gruppe, so nennen wir eine Untergruppe A von G eine *maximale Untergruppe*, wenn durch die Elemente $a_1, a_2, \ldots, a_\nu$ von A und ein in $G - A$

[1]) Satz 1, § 4.

enthaltenes Element p, also durch $\{A, p\}$ die Gruppe G völlig bestimmt ist. (D. h. G ist die kleinste $a_1, a_2, \ldots, a_\nu, p$ enthaltende Gruppe.)

Dann gilt $G \geqq A + A \,.\, q_1 + A \,.\, q_2 + \cdots + A \,.\, q_\sigma$, $A \,.\, q_1$ enthalte p, und da die Gruppe $\{A, p\}$ mit G zusammenfallen muß, so gilt $G = A + Aq_1 + \cdots + Aq_\sigma$.

Setzen wir nun $A = G_1$, so gilt das Analoge für einen Maximalteiler A_1 von G_1:

$$A = A_1 + A_1 \,.\, r_1 + A_1 \,.\, r_2 + \cdots + A_1 \,.\, r_\tau \qquad \text{usw.}$$

Wir können so fortfahrend reduzieren, bis wir auf eine einfache Gruppe (die also keinen Teiler und natürlich keinen Maximalteiler enthält) stoßen.

Denn jede endliche Gruppe muß einen Maximalteiler, der für einfache Gruppen von der Ordnung 1 ist, enthalten.

Sei nämlich A eine Untergruppe von G und $\{A, p\}$ [1]) noch nicht die Gruppe G, so ist $\{A, p\} = A_1 > A$ eine echte Untergruppe von G. $\{A_1, p_1\}$ ist dann entweder gleich G, oder wieder ein echter Teiler A_2 von G, usw.

Da die Gruppe G endlich ist, so müssen wir zu einem Ende gelangen.

I. Nachtrag [2]).

Wir bezeichnen den Komplex

(2) $\qquad (A \,.\, p) \,.\, (A \,.\, q)$, *A einfache Gruppe*, mit H_{pq}

und wollen ihn genauer untersuchen.

Alle folgenden Sätze über den Komplex H_{pq} gelten selbstverständlich auch für den Fall, daß $H_{pq} = A \,.\, (p \,.\, q)$ ist.

1. Satz: *H_{pq} hat ν oder ν^2 Elemente, wenn ν die Ordnung von A ist.*

Beweis: Wir zeigen, daß wenn H_{pq} $t < \nu^2$ Elemente hat, $t = \nu$ ist. Ist $t < \nu^2$, so gibt es zwei Elemente $(a_h \,.\, p) \,.\, (a_k \,.\, q)$ und $(a_{\bar{h}} \,.\, p) \,.\, (a_{\bar{k}} \,.\, q)$, wobei $h \neq \bar{h}$ und $k \neq \bar{k}$ ist, von der Art, daß

(3) $\qquad (a_h \,.\, p) \,.\, (a_k \,.\, q) = (a_{\bar{h}} \,.\, p) \,.\, (a_{\bar{\bar{k}}} \,.\, q)$

ist; dann ist aber zufolge Satz 1, § 4

(4) $\qquad (A \,.\, p) \,.\, (a_k \,.\, q) = (A \,.\, p) \,.\, (a_{\bar{k}} \,.\, q).$

Da aber $k \neq \bar{k}$ ist und $A \,.\, p$ durch zwei Elemente vollständig bestimmt ist, so folgt aus (4)

(5) $\quad (A \,.\, p) \,.\, (a_1 \,.\, q) = (A \,.\, p) \,.\, (a_2 \,.\, q) = \cdots = (A \,.\, p) \,.\, (A \,.\, q) = A \,.\, (p \,.\, q).$

Es ist also in diesem Falle $t = \nu$, w. z. b. w.

Bemerkung: Hat H_{pq} ν Elemente, so ist $H_{pq} = A \,.\, (p \,.\, q)$, besitzt aber H_{pq} ν^2 Elemente, so ist

(6) $\quad H_{pq} = (A \,.\, p) \,.\, (a_1 \,.\, q) + (A \,.\, p) \,.\, (a_2 \,.\, q) + \cdots + (A \,.\, p) \,.\, (a_\nu \,.\, q).$

2. Satz: *H_{pq} ist eine Gruppe.*

Beweis: Hat H_{pq} ν Elemente, so ist $H_{pq} = A \,.\, (p \,.\, q)$, demnach eine ν-gliedrige Gruppe. Wir müssen also nur zeigen, daß H_{pq} mit ν^2 Elementen eine Gruppe ist. Zufolge (6) ist

(6′) $\qquad H_{pq} = (A \,.\, p) \,.\, (a_1 \,.\, q) + \cdots + (A \,.\, p) \,.\, (a_\nu \,.\, q).$

Den Komplex

(6″) $\qquad [(A \,.\, p) \,.\, (a_r \,.\, q)] \,.\, [(A \,.\, p) \,.\, (a_s \,.\, q)]$

bezeichnen wir mit K_{rs} und zeigen, daß er weniger als ν^2 Elemente hat, demnach zufolge Satz 1 eine ν-gliedrige Gruppe von der Form

---

[1]) Mit $\{A, p\}$ ist die kleinste p und die Elemente von A enthaltende Untergruppe von G bezeichnet.

[2]) Der Nachweis $(A \,.\, p) \,.\, (A \,.\, q) =$ Gruppe der Ordnung der Gruppe A ist uns nicht gelungen. Ob dieser Satz richtig ist, steht also offen. Die Sätze des Nachtrages entstanden bei den Versuchen, unsere Vermutung zu verifizieren.

(7) $$K_{rs} = (A \,.\, p) \,.\, [(a_r \,.\, a_s) \,.\, q)] = (A \,.\, p) \,.\, (a_t \,.\, q)$$

ist, wobei

(8) $$a_r \,.\, a_s = a_t$$

ist. Es ist einerseits

(9) $$[(a_t \,.\, p) \,.\, (a_r \,.\, q)] \,.\, [(a_t \,.\, p) \,.\, (a_s \,.\, q)] = (a_t \,.\, p) \,.\, [(a_r \,.\, a_s) \,.\, q] = (a_t \,.\, p) \,.\, (a_t \,.\, q) = a_t \,.\, (p \,.\, q),$$

andererseits ist auch

(9′) $$[(a_r \,.\, p) \,.\, (a_r \,.\, q)] \,.\, [(a_s \,.\, p) \,.\, (a_s \,.\, q)] = (a_r \,.\, a_s) \,.\, (p \,.\, q) = a_t \,.\, (p \,.\, q).$$

Aus (9) und (9′) folgt, daß K_{rs} weniger als ν^2 Elemente besitzt, also von der Form (7) ist. Zufolge (6) und (7) ist

(10) $H_{pq} > K_{rs}$, d. h. H_{pq} ist eine Gruppe, w. z. b. w.

3. Satz: Für die Gruppe H_{pq} gilt neben (6) *auch die Darstellung*

(11) $$H_{pq} = A \,.\, \tau_1 + A \,.\, \tau_2 + \cdots + A \,.\, \tau_\nu, \text{ wobei } \tau_1 = p \,.\, q \text{ ist.}$$

Beweis: Es ist $A \,.\, p = A \,.\, (A \,.\, r)$ und $A \,.\, q = A \,.\, (A \,.\, s)$, demnach

(12) $$(A \,.\, p) \,.\, (A \,.\, q) = [A \,.\, (A \,.\, r)] \,.\, [A \,.\, (A \,.\, s)] \geqq A \,.\, [(A \,.\, r) \,.\, (A \,.\, s)].$$

Da aber

(13) $$[a_l \,.\, (a_h \,.\, r)] \,.\, [a_i \,.\, (a_{\bar{h}} \,.\, s)] = [a_l \,.\, (a_h \,.\, r)] \,.\, [a_l \,.\, (a_{\bar{h}} \,.\, s)]^{1}) = a_{\bar{h}} \,.\, [(a_h \,.\, r) \,.\, (a_{\bar{h}} \,.\, s)]$$

ist, so folgt daraus

(13′) $$[A \,.\, (A \,.\, r)] \,.\, [A \,.\, (A \,.\, s)] \leqq A \,.\, [(A \,.\, r) \,.\, (A. \,s)].$$

Aus (12) und (13′) folgt

$$H_{pq} = (A \,.\, p) \,.\, (A \,.\, q) = A \,.\, [(A \,.\, r) \,.\, (A \,.\, s)] \text{ und}$$

(14) $$H_{pq} = A \,.\, \sigma_1 + \cdots + A \,.\, \sigma_{\nu^2} = A \,.\, \tau_1 + \cdots + A \,.\, \tau_\nu,$$

was man ohne weiteres einsieht, indem man aus $(A \,.\, r) \,.\, (A \,.\, s)$ die Elemente σ_i der Reihe nach herausgreift und berücksichtigt, daß H_{pq} nur ν^2 Elemente hat.

4. Satz: Gilt für ein bestimmtes k von (11) *und für ein bestimmtes l von* (6) *die Beziehung*

(15) $$A \,.\, \tau_k = (A \,.\, p) \,.\, (a_l \,.\, q),$$

so ist H_{pq} ν-gliedrig und umgekehrt.

Wir beweisen zuerst den ersten Teil des Satzes. Zu diesem Zwecke bezeichnen wir mit $\vartheta(A \,.\, B)$ den Durchschnitt der beiden Komplexe A und B. Es sei H_{pq} ν^2-gliedrig, dann ist für $h = 1, 2, \ldots, \nu$

(16) $$\vartheta\,(A \,.\, \tau_1, (A \,.\, p) \,.\, (a_h \,.\, q)) \geqq a_h \,.\, (p \,.\, q), \text{ da } \tau_1 = p \,.\, q \text{ ist.}$$

Es kann also $A \,.\, \tau_k$ nicht $A \,.\, \tau_1$ sein, da $\vartheta(A \,.\, \tau_k, (A \,.\, p) \,.\, (a_h \,.\, q)) = 0$ für $h \neq l$ ist. Da aber $A \,.\, \tau_k = (A \,.\, p) \,.\, (a_l \,.\, q)$ ist, so wäre zufolge (16)

(17) $\vartheta(A \,.\, \tau_1, A \,.\, \tau_k) \geqq a_l \,.\, (p \,.\, q)$, was aber unmöglich ist, da alle $A\tau_i$, $i = 1, \ldots, \nu$ (im Falle H_{pq} ν^2-gliedrig) elementfremd sind. Es muß also H_{pq} ν-gliedrig sein, w. z. b. w.

Die Umkehrung des Satzes ist evident.

Zusatz zum Satz 4: Hat H_{pq} ν^2 Elemente, so hat eine Untergruppe $A \,.\, \tau_k$ mit einer Untergruppe $(A \,.\, p) \,.\, (a_l \,.\, q)$ genau ein Element gemeinsam.

Dies folgt aus den beiden Zerlegungen (6) und (11), denn hätten diese beiden Untergruppen zwei Elemente gemeinsam, so fielen sie als einfache Gruppen zusammen, und H_{pq} wäre ν-gliedrig.

5. Satz: Aus der Beziehung

(18) $$\vartheta(H_{pq}, H_{pr}) \neq 0$$

folgt $H_{pq} = H_{pr}$.

---

[1]) Es ist ein Element $a_{\bar{h}} \,.\, s$ in allen Gruppen $A \,.\, s$ enthalten, für welches die Relation $a_i \,.\, (a_{\bar{h}} \,.\, s) = a_l \,.\, (a_{\bar{h}} \,.\, s)$ gilt, da $A \,.\, (A \,.\, s)$ eine ν-gliedrige Gruppe ist.

Für H_{pq} resp. H_{pr} gelten die Zerlegungen

(18′) $\quad H_{pq} = A \,.\, \tau_1 + \cdots + A \,.\, \tau_\nu, \qquad H_{pr} = A \,.\, \sigma_1 + \cdots + A \,.\, \sigma_\nu,$

(wobei nicht notwendig die $A \,.\, \tau_i$ resp. $A \,.\, \sigma_i$ alle verschieden sind). Sei nach Voraussetzung

(19) $\quad (a_h \,.\, p) \,.\, (a_k \,.\, q) = (a_h \,.\, p) \,.\, (a_{\bar{k}} \,.\, r)$, so folgt daraus

(20) $\quad (A \,.\, p) \,.\, (a_k \,.\, q) = (A \,.\, p) \,.\, (a_{\bar{k}} \,.\, r).$

Wir zeigen nun, daß irgend eine Gruppe $A \,.\, \tau_i$ von H_{pq} mit einer $A \,.\, \sigma_j$ von H_{pr} identisch ist, d. h. dann, daß $H_{pq} = H_{pr}$ ist.

In der Tat! Sei $A \,.\, \tau_i$ diese Gruppe, so hat sie mit $(A \,.\, p) \,.\, (a_k \,.\, q)$ sicher ein Element x gemeinsam, also auch nach (20) mit $(A \,.\, p) \,.\, (a_{\bar{k}} \,.\, r)$. Letztere Gruppe aber hat dieses Element x ihrerseits mit einem $A \,.\, \sigma_j$ von H_{pr} gemeinsam.

Somit haben $A \,.\, \tau_i$ und $A \,.\, \sigma_j$ das Element x gemeinsam und fallen demnach zusammen.

Zuzatz zum Satz 5: Enthält die Gruppe $(A \,.\, p) \,.\, l$ *ein Element* a_i *der Gruppe* A, *so ist* $(A \,.\, p) \,.\, l \equiv A$.

In der Tat, da $A \,.\, (A \,.\, p) = A \,.\, r$ ist, so ist zufolge § 5, I. II. Hilfssatz: $A = (A \,.\, p) \,.\, s$. Die Komplexe $A \,.\, [(A \,.\, p) \,.\, h] = [(A \,.\, p) \,.\, s] \,.\, [(A \,.\, p) \,.\, l]$ und $A \,.\, A = [(A \,.\, p) \,.\, s] \,.\, [(A \,.\, p) \,.\, s] = A$ haben das Element a_i gemeinsam und sind somit identisch. Da $A \,.\, A = \nu$-gliedrig ist, so muß also der Komplex $A \,.\, [(A \,.\, p) \,.\, l$ ν-gliedrig sein, und es gilt:

$$A \,.\, [(A \,.\, p) \,.\, l] = A \,.\, A = A, \text{ d. h. } (A \,.\, p) \,.\, l = A, \quad \text{q. e. d.}$$

6. Satz: Es gilt für die Untergruppen (11) *die Relation*

(21) $\quad (A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) = A \,.\, (\tau_k \,.\, \tau_l).$

Beweis: Da H_{pq} eine Gruppe ist, so ist $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) < H_{pq}$. Wäre $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ ν^2-gliedrig, so wäre

(22) $\quad (A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) = H_{pq}$; da aber $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_k) = (A \,.\, \tau_k) < H_{pq}$

ist, so wäre

(22′) $\quad \vartheta[(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l),\ (A \,.\, \tau_k) \,.\, (A \,.\, \tau_k)] = A \,.\, \tau_k,$

also zufolge Satz 5

(22″) $\quad (A \,.\, \tau_k) \,.\, (A \,.\, \tau_l) = A \,.\, \tau_k,$

d. h. $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ müßte ν-gliedrig sein, demnach führt die Annahme, $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ sei ν^2-gliedrig, zu einem Widerspruch. Es muß das $(A \,.\, \tau_k) \,.\, (A \,.\, \tau_l)$ ν-gliedrig, also $A \,.\, (\tau_k \,.\, \tau_l)$ gleich sein, w. z. b. w.

Sei G eine Gruppe und A eine einfache Untergruppe von G, so gilt dann die Darstellung

(23) $\quad G = A \,.\, l_0 + A \,.\, l_1 + \cdots + A \,.\, l_s, \quad \text{wobei} \quad l_0 < A$

ist. Wir erinnern, daß $A \,.\, (A \,.\, p) = A \,.\, t$ gilt. Im allgemeinen braucht $(A \,.\, l_j) \,.\, (A \,.\, p) =$ ν-gliedrige Gruppe nicht zuzutreffen. Die Gruppen $A \,.\, l_j$ der Eigenschaft

(24) $\quad (A \,.\, l_j) \,.\, (A \,.\, l_h) = A \,.\, (l_j \,.\, l_h)$ für jedes $h = 0, 1, \ldots, s,$

zu denen A gehört, seien mit $A \,\tilde{.}\, l_j$ bezeichnet.

Sei (24′) $A \,\tilde{.}\, l_0 = A,\ A \,\tilde{.}\, l_1, \ldots, A \,\tilde{.}\, l_r$ die Gesamtheit dieser Gruppen, so gilt für sie

7. Satz: Die Gruppen (24′) *sind Elemente einer distributiven Gruppe* Γ. *Mit* Σ *sei die Untergruppe von* G *bezeichnet, die alle Elemente von* G *enthält, die in Elementen von* Γ *auftreten.*

Beweis: Wir zeigen, daß

(25) $\quad (A \,\tilde{.}\, l_k) \,.\, (A \,\tilde{.}\, l_h) = \widetilde{A \,.\, (l_k \,.\, l_h)}$

ist. Nach Voraussetzung gilt

$$(26)\qquad \begin{cases} (A\widetilde{.}\,l_k)\,.\,(A\,.\,l_x) = A\,.\,(l_k\,.\,l_x) \\ (A\widetilde{.}\,l_h)\,.\,(A\,.\,l_x) = A\,.\,(l_h\,.\,l_x), \end{cases}$$

speziell also

$$(25')\qquad (A\widetilde{.}\,l_k)\,.\,(A\widetilde{.}\,l_h) = A\,.\,(l_k\,.\,l_h).$$

Aus (26) schließen wir $A\widetilde{.}\,l_k = (A\,.\,l_x)\,.\,p$, $A\widetilde{.}\,l_h = (A\,.\,l_x)\,.\,q$, somit $(A\widetilde{.}\,l_k)\,.\,(A\widetilde{.}\,l_h) = (A\,.\,l_x)\,.\,(p\,.\,q)$. Nun ist $\widetilde{A\,.\,(l_k\,.\,l_h)}$ zu beweisen, d. h. $[A\,.\,(l_k\,.\,l_h)]\,.\,(A\,.\,l_x) = \nu$-gliedrig. In der Tat gilt $[A\,.\,(l_k\,.\,l_h)]\,.\,(A\,.\,l_x) = [(A\,.\,l_x)\,.\,(p\,.\,q)]\,.\,(A\,.\,l_x) = \nu$-gliedrig, w. z. b. w.

8. Satz: Es sei G eine ausgezeichnete Gruppe (siehe § 5), A eine einfache Gruppe von G der Ordnung ν und R eine A enthaltende Untergruppe von G der Ordnung ν^2. Ist

$$(26')\qquad R = A\cdot l_1 + A\cdot l_2 + \cdots + A\cdot l_\nu, \quad \textit{wobei}\quad l_1 < A \quad \textit{ist,}$$

eine Zerlegung vermittels der Gruppe A, so ist $A\,.\,l_h = A\widetilde{.}\,l_h$, $h = 1, \ldots, \nu$.

Beweis: Es sei

$$(27)\qquad G = R + R\cdot p_1 + \cdots + R\cdot p_t.$$

Aus (26′) folgt

$$(28)\qquad R\,.\,p_k = (A\,.\,l_1)\,.\,p_k + \cdots + (A\,.\,l_\nu)\,.\,p_k = (A\,.\,p_k)\,.\,(l_1\,.\,p_k) + \cdots + (A\,.\,p_k)\,.\,(l_\nu\,.\,p_k), \qquad k = 1, \ldots, t.$$

Wir zeigen, daß $R\,.\,p_k$ von der Form

$$(28')\qquad R\,.\,p_k = A\,.\,s_1^{(k)} + \cdots + A\,.\,s_\nu^{(k)}$$

ist. Da $A\,.\,(A\,.\,p_k)$ ν-gliedrig ist, so ist zufolge § 5, I. II. Hilfssatz: $A = (A\,.\,p_k)\,.\,\sigma$. Betrachten wir jetzt die beiden Komplexe

(29) $A\,.\,(A\,.\,p_k) = [(A\,.\,p_k)\,.\,\sigma]\,.\,(A\,.\,p_k)$ und $A\,.\,[(A\,.\,p_k)\,.\,(l_r\,.\,p_k)] = [(A\,.\,p_k)\,.\,\sigma]\,.\,[(A\,.\,p_k)\,.\,(l_r\,.\,p_k)]$, $r = 1, \ldots, \nu$. Sie sind beide in der Gruppe $R\,.\,(R\,.\,p_k) = R\,.\,p_t$ enthalten, demnach müssen sie zufolge Satz 5 entweder zusammenfallen, oder beide ν-gliedrig sein. Da aber der erste Komplex ν-gliedrig ist, so ist es auch der zweite, und die Gruppe $(A\,.\,p_k)\,.\,(l_r\,.\,p_k) = (A\,.\,l_r)\,.\,p_k$ ist von der Form $A\,.\,s_\nu^{(k)}$, d. h. es ist

$$R\,.\,p_k = A\,.\,s_1^{(k)} + \cdots + A\,.\,s_\nu^{(k)}.$$

Ist $A\,.\,\tau$ irgendeine Untergruppe von G, so fällt sie zufolge (27) und (28′) mit einer Untergruppe, z. B. $A\,.\,s_r^{(k)}$, zusammen. Indem man jetzt die beiden Komplexe

$$(30)\qquad A\,.\,(A\,.\,s_r^{(k)}) \text{ und } (A\,.\,l_k)\,.\,(A\,.\,s_r^{(k)}), \quad k = 1, \ldots, \nu$$

betrachtet, schließt man auf dieselbe Weise wie vorher, da $A\,.\,(A\,.\,s_r^{(k)})$ ν-gliedrig ist, daß auch $(A\,.\,l_k)\,.\,(A\,.\,s_r^{(k)})$ ν-gliedrig ist, d. h. daß $A\,.\,l_k = A\widetilde{.}\,l_k$ ist, w. z. b. w.

9. Satz: Jede ausgezeichnete Gruppe G ist entweder identisch mit Σ[1]) oder enthält mindestens ν Untergruppen $A\widetilde{.}\,l_k$.

Beweis: Ist für jedes $(A\,.\,p)$ und $(A\cdot q)$

$$(31)\qquad (A\,.\,p)\,.\,(A\,.\,q) = A\,.\,(p\,.\,q), \quad \text{so ist}\quad G \equiv \Sigma.$$

Ist das nicht der Fall, so existiert mindestens eine Untergruppe $A\,.\,p$, so daß $(A\,.\,p)\,.\,(A\,.\,q) = H_{pq}$ ν^2-gliedrig ist. Es sei l ein Element von G, von der Art, daß

$$(32)\qquad [a_1\,.\,(p\,.\,q)]\,.\,l = a_i, \quad (a_1, a_i \text{ Elemente von } A).$$

Die Gruppe $(H_{pq})\,.\,l$ enthält zufolge Zusatz zu Satz 5 die Gruppe A, es ist also

$$(33)\qquad (H_{pq})\,.\,l = A + A\,.\,\varrho_1 + \cdots + A\,.\,\varrho_{\nu-1}.$$

Die Gruppe $(H_{pq})\,.\,l$ hat demnach die Eigenschaften der Gruppe R des Satzes 8, demnach ist $A\,.\,\varrho_k = A\widetilde{.}\,\varrho_k$, $k = 1, 2, \ldots, \nu$, q. e. d.

---

[1]) d. h. jede Untergruppe $A\,.\,p$ der Gruppe G ist eine $A\widetilde{.}\,p$-Untergruppe.

Bemerkung: Ist G eine ausgezeichnete Gruppe von der Ordnung N, wobei $N = \prod_{i=1}^{n} p_i$ ist und p_i Primzahlen sind, von der Art, daß $p_i \neq p_k$ ist, wenn $i \neq k$ ist, so gilt dann für die Gruppe G der Relation

$$(34) \qquad (A \,.\, p) \,.\, (A \,.\, q) = A \,.\, (p \,.\, q)$$

für jede einfache Untergruppe A von G.

In der Tat! Wäre das nicht der Fall, so müßte $(A \,.\, p) \,.\, (A \,.\, q) = H_{pq}$ eine ν^2-gliedrige Gruppe sein. Da G eine ausgezeichnete Gruppe ist, so müßte dann zufolge § 4, Satz 1 N durch ν^2 teilbar sein, was gegen die Voraussetzung ist. Es gilt demnach (34). Gilt aber die Beziehung (34) für alle einfachen Untergruppen in G, so gilt sie auch für alle Untergruppen in G überhaupt (wie man leicht zeigen kann).

Da jede symmetrische distributive Gruppe G von der Ordnung $N = \prod_{i=1}^{n} p_i$, wobei N durch 3 nicht teilbar ist, eine ausgezeichnete Gruppe ist, so gilt für symmetrische Gruppen dieser Eigenschaften die Beziehung (34).

II. Nachtrag: Einiges über die Struktur distributiver Gruppen.

Sei $G = \{a_1, a_2, \ldots, a_\nu\}$ eine distributive Gruppe, so bilden wir aus zwei Elementen a_1 und a_2 den folgenden l-Cyklus (links-Cyklus) $a_1 \,.\, a_2 = a_3$, $a_1 \,.\, a_3 = a_4, \ldots, a_1 \,.\, a_{h-1} = a_h$. $a_1, a_2, \ldots, a_h$ sollen alle verschieden sein, dagegen möge $a_1 \,.\, a_h$ bereits in der Reihe $a_1, a_2, \ldots, a_h$ enthalten sein.

$a_1 \,.\, a_h$ muß von a_1 und a_h verschieden sein, ist also $a_1 \,.\, a_h = a_i$, so muß $i > 1$ sein, wir behaupten $i = 2$; wäre $i > 2$, so folgt aus

$$a_1 \,.\, a_h = a_i \text{ und } a_h = a_1 \,.\, a_{h-1},\ a_i = a_1 \,.\, a_{i-1}\,,$$

daß $a_1 \,.\, a_{h-1} = a_{i-1}$; also müßte bereits $a_1\, a_{h-1} = a_h = a_{i-1}$ in der Reihe $a_1, a_2, \ldots, a_{h-1}$ enthalten sein, gegen die Voraussetzung.

Der Cyklus lautet demnach:

$$(\alpha) \qquad a_1, a_2, a_3 = a_1 \,.\, a_2, \quad a_4 = a_1 \,.\, a_3, \quad a_h = a_1 \,.\, a_{h-1}, \quad a_2 = a_1 \,.\, a_h.$$

Zwischen a_1 und a_2 besteht dann die Relation:

$$a_1^{h-1} \,.\, a_2 = a_2.$$

Der Gleichung $a_1^{h-1} \,.\, x = x$ genügen die Elemente einer Untergruppe, die die Elemente des Cyklus (α) enthält.

Zwischen je zwei Elementen a, b dieser Untergruppe (§ 2) besteht dann die Relation

$$a^{h-1} \,.\, b = b, \text{ also gilt auch } a_2^{h-1} \,.\, a_1 = a_1 \text{ usw.}$$

Wir nennen $h - 1$ den Grad des l-Cyklus a_1, a_2. Sei $A\{a_1\, a_2, \ldots, a_\nu\}$ eine einfache Gruppe, so ist der Grad G des l-Cyklus je zweier Elemente a_p und a_q, $a_p \neq a_q$ eine der einfachen Gruppe charakteristische Zahl, d. h. dieser l-Grad ist von der besonderen Wahl der Elemente a_p und a_q unabhängig.

Beweis: Je zwei Elemente von A, a_p, a_q, haben einen bestimmten l-Grad g_{pq}; unter den ganzen Zahlen g_{pq} muß es eine kleinste geben. a_i und a_k sei eine Kombination, deren Cyklusgrad g sei, dann gilt $a_i^g \,.\, a_k = a_k$. Die Elemente x, die die Gleichung $a_i^g \,.\, x = x$ lösen, bilden eine Untergruppe von A die, da sie a_i und a_k enthält, mit A, da A einfach ist, zusammenfallen muß. Demnach gilt

$$a_p^g \,.\, a_q = a_q \text{ für alle Elemente von } A,$$

d. h. je zwei Elemente a_p und a_q haben den Cyklusgrad g, q. e. d.

Sei A eine einfache Gruppe, N ihre Ordnung und g ihr l-Cyklusgrad. Dann bilden wir mit a_1 und a_2 den Cyklus

$$(\alpha) \qquad a_1, a_2, a_3 = a_1 \cdot a_2, \ldots, a_{g+1} = a_1 \cdot a_g \ (a_2 = a_1 \cdot a_{g+1}).$$

Sind mit $a_1, a_2, \ldots, a_{g+1}$ noch nicht alle Elemente erschöpft, so sei a_{g+2} ein noch nicht in (α) enthaltenes Element. Wir bilden

$$(\beta) \qquad a_1, a_{g+2}, a_{g+3} = a_1 \cdot a_{g+2}, \ldots, a_{2g+1} = a_1 \cdot a_{2g} \ (a_{g+2} = a_1 \cdot a_{2g+1}).$$

Wäre $a_i = a_{g+k}$, $i, k = 2, 3, \ldots, g+1$, so folgte

$$a_1 \cdot a_i = a_{i+1} = a_1 \cdot a_{g+k} = a_{g+k+1} \qquad \text{usw.},$$

endlich $a_{g+2} = a_l$, gegen die Voraussetzung.

Somit sind die Reihen (α) und (β) vom gemeinsamen Element a_1 abgesehen teilerfremd.

Sei durch (α) und (β) A noch nicht erschöpft, so bilden wir mit a_1, a_{2g+2} einen neuen Cyklus usw., bis A erschöpft ist. Jede Reihe (α), (β) ... enthält $g+1$ Elemente, somit gilt $N = \sigma g + 1$, wobei σ ganze Zahl ist, oder

$$N \equiv 1 \mod g.$$

Satz: Ist N die Ordnung und g der Cyklusgrad einer einfachen Gruppe, so gilt

$$N \equiv 1 \mod g.$$

Das gleiche gilt natürlich für den r-Grad (Grad des rechtsseitigen Cyklus); wir haben nur die Verknüpfung

$$a_i \circ a_k = a_k \cdot a_i$$

anstelle von $a_i \cdot a_k$ zu betrachten, für die das System $A\{a_1, a_2, \ldots, a_\nu\}$ ebenfalls eine distributive Gruppe bildet.

Im allgemeinen ist der l-Grad vom r-Grad verschieden.

Sei $A\{a_0, a, \ldots, a_\nu\}$ ein System, dessen Elemente einen einzigen Cyklus bilden:

$$a_0, a_1, a_2 = a_0 \cdot a_1, a_3 = a_0 \cdot a_2, \ldots, a_\nu = a_0 \cdot a_{\nu-1} \ (a_0 \cdot a_\nu = a_1).$$

Wir zeigen dann, daß aus der Gültigkeit der Axiome I und II und der linksseitigen Distributivität die rechtsseitige Distributivität für das System A folgt. Da für solche Systeme auch die Homogenitätseigenschaft gilt, ist der Beweis gebracht, sobald

$$(a_i \cdot a_k) \cdot a_0 = (a_i \cdot a_0) \cdot (a_i \cdot a_0)$$

gilt. Wir bezeichnen mit a_ϱ das Element, für das

$$a_0 \cdot a_1 = a_\varrho \cdot a_0$$

gilt. Durch linksseitige Verknüpfung mit a_0 erhalten wir

$$(\alpha) \quad \left\{ \begin{array}{l} a_0 \cdot a_{[t]} = a_{[\varrho+t-1]} \cdot a_0, \quad a_{\varrho+t-1} = a_k \text{ gesetzt}, \quad t = k+1-\varrho \\ a_0 \cdot a_{[k+1-\varrho]} = a_{[k]} \cdot a_0 \end{array} \right\}.$$

Dabei ist $[i]$ jene Zahl der Reihe $1, 2, \ldots, \nu$, für die

$$[i] \equiv i \mod \nu$$

gilt. Nun folgt aus (α), (β)

$$(a_t \cdot a_0) \cdot (a_s \cdot a_0) = [a_0 \cdot a_{[t+1-\varrho]}] \cdot [a_0 \cdot a_{s+1-\varrho]}] = a_0 \cdot [a_{[t+1-\varrho]} \cdot a_{[s+1-\varrho]}]$$
$$= a_0 \cdot a_\mu = a_{[\varrho+\mu-1]} \cdot a_0,$$

wobei

$$a_\mu = a_{[t+1-\varrho]} \cdot a_{[s+1-\varrho]} \qquad \text{ist.}$$

Linksseitig $(\varrho - 1)$-mal mit a_0 verknüpft ergibt dies:

$$a_t \cdot a_s = a_{[\mu+\varrho-1]}, \text{ somit lautet } (\beta):$$
$$(a_t \cdot a_0)(a_s \cdot a_0) = (a_t \cdot a_s) \cdot a_0, \quad \text{q. e. d.}$$

Eingegangen im November 1927.